

1 UNITED STATES DISTRICT COURT
2 FOR THE NORTHERN DISTRICT OF OHIO
3 EASTERN DIVISION

4 - - - - -

5 UNITED STATES OF AMERICA,)
6 Plaintiff,)
7 vs.) Case No. 1:16CR224
8 BOGDAN NICOLESCU,)
9 RADU MICLAUS,)
10 Defendants.)

11 - - - - -

12
13 CONTINUED TRANSCRIPT OF TRIAL PROCEEDINGS HAD
14 BEFORE HONORABLE JUDGE PATRICIA A. GAUGHAN, JUDGE
15 OF SAID COURT, ON WEDNESDAY, APRIL 3RD, 2019,
16 COMMENCING AT 10:00 O'CLOCK A.M.

17 - - - - -

18 Volume 8, Pages 1379 through 1583
19 - - - - -

20
21
22
23 Court Reporter: GEORGE J. STAUDUHAR
24 801 W. SUPERIOR AVE.,
25 SUITE 7-184
CLEVELAND, OHIO 44113
(216) 357-7128

1 APPEARANCES:

2 On behalf of the Government:

3 OFFICE OF THE U.S. ATTORNEY
4 BY: DUNCAN T. BROWN, AUSA
5 BRIAN M. McDONOUGH, AUSA
6 801 West Superior Ave., Suite 400
7 Cleveland, OH 44113

8 and

9 U.S. DEPARTMENT OF JUSTICE - CRIMINAL DIVISION
10 BY: BRIAN L. LEVINE, SENIOR COUNSEL
11 1301 New York Avenue, Suite 600
12 Washington, DC 20530

13 On behalf of Defendant Bogdan Nicolescu:

14 LAW OFFICE OF MICHAEL J. GOLDBERG
15 BY: MICHAEL J. GOLDBERG, ESQ.
16 323 Lakeside Place, Suite 450
17 Cleveland, OH 44113

18 On behalf of Defendant Radu Miclaus:

19 LIPSON O'SHEA
20 BY: MICHAEL J. O'SHEA, ESQ.
21 110 Hoyt Block Building
22 700 West St. Clair Avenue
23 Cleveland, OH 44113
24
25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

I N D E X

<u>WITNESSES:</u>	<u>DIRECT</u>	<u>CROSS</u>	<u>REDIRECT</u>	<u>RECROSS</u>
Tiberiu Danet			1450	
By Mr. Goldberg		1384		1452
By Mr. O'Shea		1434		1455
Bogdan D. Vaduva	1457			
By Mr. Goldberg		1593		
By Mr. O'Shea		1508		
Ryan Macfarlane	1514			

P R O C E E D I N G S

THE COURT: Please be seated. Good morning, ladies and gentlemen.

Ladies and gentlemen as you can see, Juror No. 9, Ms. Diamond, is no longer here. I apologize for the delay this morning, but I, along with counsel, had to make a very critical decision, and that is, do we proceed, or do we simply recess until she can come back?

We made the decision to proceed because we still have an alternate that can now and is now Juror No. 9, but unfortunately, for the rest of you, that means that if anyone else gets sick, we literally are going to have to recess the trial until that person is well again and can come back because, as you can see, we cannot afford to lose another juror.

We also made the decision because we are close to the end of the trial, and we thought we would take the risk that all twelve of you will stay healthy enough to be able to make it in.

I am permitted to represent to you that we anticipate all of the evidence will be concluded sometime on Tuesday, and again, for those reasons, we made the critical decision to not wait for Ms. Diamond to get better because we don't want to impose any more time on

1 the rest of you. We didn't think that would be fair.

2 But I have to reiterate, if one more person
3 becomes ill, I am going to have to impose upon the rest
4 of you, which means we will all have to literally sit and
5 wait until that juror gets better; recess the trial, be
6 it a day, two days, three days, et cetera, we have no
7 choice.

8 So I just need to give you the heads up. If
9 it happens again, we are going to take a recess as long
10 as it takes to get that juror back.

11 I apologize for the delay, but we really had
12 to do some good, hard thinking on how to proceed here. I
13 have never had a situation where we have lost four jurors
14 within a little over a week time. So this is new for all
15 of us.

16 On behalf of the Government, are you
17 satisfied with this solution?

18 MR. BROWN: Yes, your Honor. Thank you very
19 much.

20 THE COURT: On behalf of Mr. Nicolescu?

21 MR. GOLDBERG: After consultation with my
22 client, yes, we are.

23 THE COURT: On behalf of Mr. Miclaus?

24 MR. O'SHEA: Yes, your Honor.

25 THE COURT: Cross examination, Mr. Goldberg?

Mr. Tiberiu Danet - Cross

1 CROSS EXAMINATION

2 BY MR. GOLDBERG:

3 Q. I am Mike Goldberg, and I have questions about your
4 testimony. If you don't understand a question, it will
5 be my fault, and I will try to rephrase it.

6 You were arrested on September 28th, 2016,
7 correct?

8 A. Yes.

9 Q. And you have been in jail or prison or custody ever
10 since then, right?

11 A. Yes.

12 Q. And during that period — when was your first Court
13 appearance. Do you remember?

14 A. The arraignment was on December 14th or 15th of
15 2016.

16 Q. Here?

17 A. Yes.

18 Q. In Ohio, but in Romania, did you go to Court in
19 Romania?

20 A. Yes. I think it was one day after getting arrested
21 or two days.

22 Q. And you had a lawyer then?

23 A. Yes.

24 Q. And you had a lawyer since you got here in the
25 United States?

Mr. Tiberiu Danet - Cross

1 A. Yes.

2 Q. And you continue to have attorneys, correct?

3 A. Yes.

4 Q. Okay. And you pled guilty last summer, or I'm
5 sorry, in the fall in this case, correct?

6 A. Yes.

7 Q. And you had a sentencing that had been scheduled,
8 but it has since been continued a couple times,
9 right?

10 A. I think it was continued once.

11 Q. Okay. And that's to move it beyond the date of the
12 trial so that the Government can hear how you do in the
13 courtroom before they give you any credit for your
14 testimony, correct?

15 A. No. The decision was made by my attorney.

16 Q. Oh, it was your attorney's decision?

17 A. Yeah.

18 Q. So what you say in the courtroom would have no
19 bearing on what kind of sentence would be recommended by
20 the Government?

21 MR. BROWN: Objection.

22 BY MR. GOLDBERG:

23 Q. Is that your understanding?

24 A. Yes, it is my understanding.

25 Q. That the Government doesn't have any —

Mr. Tiberiu Danet - Cross

1 THE COURT: I'm sorry. I just saw
2 objection, but I didn't hear it.

3 MR. BROWN: And I noticed the microphone was
4 not on, but I objected, and I will object to this
5 question, your Honor.

6 THE COURT: Overruled.

7 BY MR. GOLDBERG:

8 Q. You don't think the Government has any say in your
9 sentencing?

10 A. I know that the Government can make a position
11 within the range of the plea.

12 Q. Right. And if they are —

13 A. Like my attorneys, too.

14 Q. And if they are satisfied with what you say in
15 Court, they can recommend nine years, and if they are
16 unsatisfied, they can recommend the high end, which is
17 what, 12?

18 A. They can recommend the high end anyway, too.

19 Q. Okay. So you testified yesterday that you met
20 Mr. Nicolescu again because you knew him through your
21 brother and didn't really have contact with him while you
22 were in school until around 2007 or '8, correct?

23 A. Yes. I think it was around 2007.

24 Q. Okay. And at that point, where were you
25 living?

Mr. Tiberiu Danet - Cross

1 A. With my parents.

2 Q. Okay. And were they in an apartment or a
3 house?

4 A. Yes, in an apartment.

5 Q. The same apartment where you were living when you
6 were arrested?

7 A. No.

8 Q. You were living with your parents and who else?

9 A. My brother.

10 Q. Okay. And at that time, was your brother engaged in
11 internet fraud?

12 A. No. He got engaged in internet fraud probably
13 around —

14 Q. The question was: Was he engaged in internet fraud
15 in 2008 when you met Mr. Nicolescu?

16 A. It happened around the same time.

17 Q. Okay. So when you met Mr. Nicolescu in 2008 and
18 started talking to him, were you engaged in internet
19 fraud at that time?

20 A. No. But again, this was 2007, not '8.

21 Q. 2007. Thank you for correcting me.

22 So you didn't commit any internet fraud
23 crimes, and your brother didn't commit any internet
24 crimes until you both met Mr. Nicolescu in 2007?

25 A. Even though I was living —

Mr. Tiberiu Danet - Cross

1 A. That's a yes or no.

2 MR. BROWN: Objection, your Honor.

3 THE COURT: Sustained. Can I have one
4 moment?

5 A. The question again?

6 THE COURT: One moment.

7 BY MR. GOLDBERG:

8 Q. When you met Mr. Nicolescu in 2007, you had not
9 committed any internet crime or any crimes up to that
10 point, correct?

11 A. Yes, that's right.

12 Q. And when your brother met Mr. Nicolescu in 2007, was
13 it at the same time?

14 A. I don't know when my brother met Mr. Nicolescu. As
15 far as I know, they had been classmates in high school.
16 I was not around my brother all the time.

17 Q. But your brother engaged in internet crime as well
18 after meeting Mr. Nicolescu, correct?

19 A. Yes. But I can't say when that started.

20 Q. Okay. But not before that as far as you know,
21 right?

22 A. As far as I know, yes.

23 Q. And you were sharing a room at the time in your
24 apartment?

25 A. No.

Mr. Tiberiu Danet - Cross

1 Q. With your brother?

2 A. No. We had two rooms.

3 Q. Okay. So I want to ask you about some things right
4 at the end of your testimony yesterday. You were asked
5 by Mr. Brown about the central control server. Is that
6 the right term?

7 A. Yes.

8 Q. And you were asked who had log-ins for that,
9 right?

10 A. Yes.

11 Q. And you indicated three or four people, and I think
12 you eventually settled on four, right?

13 A. Yes.

14 Q. And we are talking about — do you know what company
15 hosted that server?

16 A. That server changed location multiple times.

17 Q. It was always one server, but it moved around?

18 A. Yes.

19 Q. You said that four people had log-in credentials,
20 and log-in credentials allows you to go on to that server
21 and work in a work space, correct?

22 A. Allows you to log into the server and modify
23 whatever you want to.

24 Q. Do whatever you want, right?

25 A. Yes.

Mr. Tiberiu Danet - Cross

1 Q. And then, you were shown an exhibit, Government's
2 Exhibit 2203. Do you remember seeing that?

3 MR. GOLDBERG: I am going to approach if I
4 may?

5 THE COURT: Sure.

6 BY MR. GOLDBERG:

7 Q. Do you remember seeing that?

8 A. Yes. It is on the screen.

9 Q. So when you were asked without seeing the exhibit —
10 had you seen this exhibit before your testimony?

11 A. I don't understand. It was on the screen yesterday,
12 too.

13 Q. Okay. I am going to backup because I started one
14 question and finished with another.

15 Prior to your testimony yesterday, had you
16 seen Exhibit 2203?

17 A. Yes.

18 Q. And you had gone over it with the prosecutors prior
19 to your testimony?

20 A. Gone over what exactly?

21 Q. Exhibit 2203.

22 A. I was shown the exhibit.

23 Q. Okay. Now, this exhibit shows the individuals that
24 have access and work space on the control server,
25 correct?

Mr. Tiberiu Danet - Cross

1 A. No. This shows the individuals that were using AOL
2 and Yahoo actually to create automatically for this
3 server.

4 Q. Okay. Now, doesn't it say "work spaces" at the
5 top?

6 A. Yes. It says work space.

7 Q. That's the — that is a particular part of the
8 server, is the work space, correct?

9 A. It is a folder —

10 Q. Right.

11 A. — in the server.

12 Q. It is inside the server?

13 A. Yes.

14 Q. And in order to get into the work space, you need
15 log-in credentials, correct?

16 A. No. The log-in credential was only one, actually
17 two, two log-in credentials. One was the root. Whoever
18 had the root password had access to everything in the
19 server.

20 Q. Okay.

21 A. And pretty much the same where another account,
22 which is used — whoever had the work space in the
23 accounts are not related and the log-in.

24 Q. Okay. The log-ins and the work spaces are not
25 related is your testimony?

Mr. Tiberiu Danet - Cross

1 A. Yes.

2 Q. But we can agree that the name Natiune, Raul,
3 Sasha and TRX all had work spaces on the computer,
4 correct?

5 A. Yes. They are folders.

6 Q. They could go on to the command or the central
7 command server, correct?

8 A. These are names of folders, not names of
9 users.

10 Q. Yeah, but they are on the — these are on the
11 server?

12 A. Yes. They are on the server.

13 Q. So we can agree those individuals also had
14 credentials to access these files on the server?

15 A. No. You are mistaken.

16 Q. So they can just go on the server and was open to
17 whose ever address and go into the —

18 A. You didn't have to log in to the server to be able
19 to use something from a web page. Whatever was available
20 on the server — you could go online to a specific
21 address and access something from over there. You didn't
22 have to log in to the server to have access from a web
23 browser.

24 Q. Okay. So you are saying —

25 A. And this is how these people were accessing the

Mr. Tiberiu Danet - Cross

1 respective folders from within the web browser.

2 Q. Okay. So they could just freely get on to a work
3 space on a server to a web browser?

4 A. Yes.

5 Q. They didn't need the credentials to change
6 files —

7 A. Exactly.

8 Q. — on the server itself.

9 A. Yes.

10 Q. And one of those persons was your brother under the
11 name of Raul, correct?

12 A. Yes.

13 Q. And his name is Valentin Danet, correct?

14 A. Yes.

15 Q. And it is your testimony that Mr. Danet was —
16 you don't know when he started engaging in fraud,
17 but eventually, he was engaging in internet fraud,
18 correct?

19 A. Yes.

20 Q. Now, you testified about ways that members of this
21 conspiracy communicated with each other, and you talked
22 about Jabber. I don't believe I heard you talk about
23 WhatsApp.

24 Did you communicate with anyone else that
25 was engaged in the Bayrob Group over WhatsApp?

Mr. Tiberiu Danet - Cross

1 A. No.

2 Q. Never?

3 A. I had — I didn't have WhatsApp installed on mine at
4 least in 2016. I had it at one time.

5 Q. But it was not something that was considered secure
6 enough to use, right?

7 A. Yes.

8 Q. What about Hangouts? Hangouts, do you know what
9 that is?

10 A. It is a service by Google.

11 Q. Is it similar to WhatsApp?

12 A. It looks like WhatsApp, but the underlying protocol
13 is actually Jabber, so it more depends on how you look at
14 it.

15 Q. Okay.

16 A. It looks like WhatsApp but works differently under
17 the hood.

18 Q. It is similar to Jabber, but it looks the same?

19 A. Yeah, Jabber but looks like WhatsApp.

20 Q. Did you ever communicate with anybody in the Bayrob
21 Group using Hangouts?

22 A. I might have did. I was not using it regularly, but
23 I have been.

24 Q. But it was not something that was regularly —

25 A. No.

Mr. Tiberiu Danet - Cross

1 Q. Okay. So your degrees you mentioned, your degrees I
2 thought you said format, either format or formatting,
3 something to that effect?

4 A. Computer science.

5 Q. Computer science?

6 A. Yeah.

7 Q. Okay. So that's what it is, you have a Master's in
8 computer science?

9 A. Yes.

10 Q. And your focus — or at least something that you
11 have an advanced degree — is in databases, correct?

12 A. Yes.

13 Q. And databases are essential to the whole Bayrob
14 function?

15 A. Yes.

16 Q. Your function within the Bayrob Group was to create
17 databases and ways of using database information,
18 correct?

19 A. I did that, too, but it was not my responsibility.
20 I was not the only one doing that.

21 Q. Okay. You created the .PHP pages, right?

22 A. Some of them.

23 Q. HTML pages, right?

24 A. Yes.

25 Q. You created some false eBay listings, correct?

Mr. Tiberiu Danet - Cross

1 A. Yes.

2 Q. And did you mention how many of those you did where
3 you actually created the ad, the listing itself?

4 A. How many listings I made?

5 Q. Uh-huh.

6 A. I can't remember. No, I didn't mention that.

7 Q. You talk about creating software or code that could
8 scrap credit card data, web history, users' names,
9 passwords, processing data, correct?

10 A. Yeah. I mentioned processing data such as web
11 history, but as far as the software goes, I wasn't the
12 only one.

13 Q. Okay. Well, I understand that.

14 A. Yes.

15 Q. But you created — you did these essential functions
16 for the Bayrob Group, correct?

17 A. They are far from essential.

18 Q. Pardon me?

19 A. They are far from essential.

20 Q. They are far from essential?

21 A. Yes.

22 Q. So if you didn't do the actions that you have
23 admitted to doing —

24 A. No. I meant what you mentioned right now.

25 Q. Okay. Those actions aren't essential?

Mr. Tiberiu Danet - Cross

1 A. Like the web history and, yeah, that is, it didn't
2 help the network run.

3 Q. Let's talk about things essential like the credit
4 cards, right? That's essential?

5 A. It is and isn't. You could say the database is more
6 essential, but the credit cards at some point were bought
7 for \$3, \$5 apiece, and that was not essential. If you
8 had that, you could buy that.

9 Q. Okay. So when you talked about classic Bayrob fraud
10 at the beginning of your testimony yesterday —

11 A. Yes.

12 Q. — and you talked about creating web pages, that
13 would allow the theft of monies from eBay customers
14 through a phony web page, correct?

15 A. Yes.

16 Q. And you created that. You built that.

17 A. I created the page itself, the way the page was
18 displayed to the users; which was the really hard part, I
19 didn't do that.

20 Q. But without the web page, it doesn't happen,
21 right?

22 A. Yeah. You could —

23 Q. You could say that. You got to agree with me on
24 that?

25 A. You could say that. If you don't have the 1

Mr. Tiberiu Danet - Cross

1 percent, yes, it doesn't work.

2 Q. You also instructed individuals in the Bayrob Group
3 on how to spam. I think I saw an e-mail you sent with
4 that header, right?

5 A. Yes. It was in Europe.

6 Q. Is that something you had any special understanding
7 of or training in or practice?

8 A. No. I had just created the interface that allowed
9 the web interface that helped run a whole engine behind
10 the scenes.

11 Q. Uh-huh.

12 A. That did the spamming. I just created a web
13 interface and sent an e-mail on how to use the web
14 interface, which has nothing to do with how the spam
15 works in the background, which was done by somebody
16 else.

17 Q. Okay. But these are the things that you did and
18 contributed to the Bayrob Group, correct?

19 A. Yes.

20 Q. And you got money out of this scheme over the course
21 of nine years, eight years?

22 A. Yes. I tried to answer this question yesterday,
23 too, but when you say "nine years," you make it seem that
24 it has been going on for everyday for the nine years.

25 Q. Let's say it this way —

Mr. Tiberiu Danet - Cross

1 A. There were breaks of years in this nine years.

2 Q. — there were breaks of entire years?

3 A. For me, yes.

4 Q. Okay. Which entire years?

5 A. For example, again —

6 Q. Tell me what years. Just tell me what years you
7 didn't engage in this fraud. I don't want examples. I
8 want years, numbers.

9 A. Yeah, I didn't say years like one continuous year.
10 I said out of the nine years, there were probably a total
11 of three or four like added months, maybe three —

12 Q. Three or four years if you add up the months. Is
13 that what you are saying?

14 A. Yes.

15 Q. So out of the nine years, if you added the months
16 you were involved, they would add up to four years?

17 A. Less than four.

18 Q. Less than four. Okay.

19 So there should be big breaks —

20 A. Yeah.

21 Q. Well, let me finish my question.

22 There should be big breaks in the evidence
23 of when you were involved and when you weren't involved,
24 correct?

25 MR. BROWN: Objection.

Mr. Tiberiu Danet - Cross

1 THE COURT: Overruled.

2 A. Yes.

3 THE COURT: You can answer that, sir.

4 A. There are — when you say "involved" —

5 Q. When you were working? You said you weren't
6 actually involved.

7 A. When you say involved, it doesn't mean if I sent an
8 e-mail or logged in on the e-mail I was doing anything.

9 Q. Okay. So let me get this straight.

10 You may not have been involved in this
11 conspiracy for half the time, but there still may be some
12 e-mails to the members during the time you weren't
13 involved. Is that what you are saying?

14 A. First of all, I said —

15 Q. Just answer what I am saying, or no it is not.

16 A. You are twisting my words. I said half the time, I
17 said three out of the nine. That's one third of the
18 time.

19 Q. Okay. Well, you said four or more is what you just
20 said now. So that's half of the time. If you want
21 to say a third of the time, that's fine. Answer my
22 question.

23 You still communicated with members of the
24 conspiracy, even though you weren't, quote, involved?

25 A. Not all the time, no.

Mr. Tiberiu Danet - Cross

1 Q. Okay. So you made money out of the scheme?

2 A. Yes.

3 Q. And you were living with your parents most of the
4 time?

5 A. In the beginning.

6 Q. When did you move out from your parents' home?

7 A. Probably around 2008 or '9.

8 Q. So at the beginning, you were living with your
9 parents and then moved out. Where did you move?

10 A. To an apartment.

11 Q. The apartment where you were arrested?

12 A. No.

13 Q. Where was this apartment?

14 A. In Bucharest.

15 Q. Okay. And was it one you rented, or was it owned by
16 a member of your family?

17 A. It was rented.

18 Q. Okay. And when you were arrested, you were living
19 in an apartment that was owned by a member of your
20 family?

21 A. Yes.

22 Q. Who was it owned by?

23 A. My mother. She had inherited from her mother.

24 Q. And how long had you been living there?

25 A. Probably something like five years.

Mr. Tiberiu Danet - Cross

1 Q. Okay. So we could say safely about 2011 you moved
2 in there?

3 A. Probably.

4 Q. Okay. And you were paid — you made money in
5 bitcoin with your involvement —

6 MR. BROWN: Objection.

7 THE COURT: Let me hear the question.

8 BY MR. GOLDBERG:

9 Q. You made money in the Bayrob scheme in bitcoin, paid
10 in bitcoin or paid in cash, correct?

11 THE COURT: Overruled.

12 A. Yes.

13 Q. And it didn't matter which to you as long as you got
14 paid, right?

15 A. For the longest time.

16 Q. It didn't matter which way you got paid?

17 A. Yeah, because in the beginning, there was no
18 bitcoin.

19 Q. When it became bitcoin, then it didn't matter?

20 A. No. It became like four years after bitcoin was
21 created.

22 Q. Okay. So when you got paid, you didn't just keep
23 that money in your apartment. You gave it to your
24 parents to put in their bank accounts, correct?

25 A. No.

Mr. Tiberiu Danet - Cross

1 Q. That would be ridiculous, right? That would be
2 silly?

3 A. I did not do that.

4 Q. No. Did you provide any information to the
5 Government about where the money went that you realized
6 from this criminal activity?

7 A. Yes.

8 Q. Okay. And where did you tell them it went?

9 A. Well, more than a hundred thousand Euros went to
10 Nicolescu's father

11 Q. Okay.

12 A. The rest of it I spent. I even loaned to Nicolescu
13 when he was short on cash.

14 Q. Okay.

15 A. And of course, I bought a car. I bought —

16 Q. None of it got stashed away?

17 A. Some of it was even seized during my arrest.

18 Q. Some of it. None of it got stashed away? You had a
19 girlfriend when you got arrested?

20 A. Yes.

21 Q. She is your girlfriend?

22 A. Yes.

23 Q. She was living in your apartment?

24 A. Yeah.

25 Q. She is waiting for this to be over for you to get

Mr. Tiberiu Danet - Cross

1 out of jail and come back to her?

2 A. Yes.

3 Q. She didn't have any of your money?

4 A. No.

5 Q. So — and you agreed to forfeit any money that you
6 made as a result of this scheme as part of your plea
7 deal, right?

8 A. Yes.

9 Q. And other than the money that was seized at the time
10 of your arrest, what funds have you turned over to the
11 Government or identified that were part of your
12 forfeiture?

13 A. I have tried to decrypt my containers that contained
14 funds without success.

15 Q. You have tried?

16 A. Yes.

17 Q. Okay. So in the course of your discussions with the
18 Government, you indicated that you had up to 200 bitcoin
19 somewhere encrypted in an encrypted partition in your
20 computer, right?

21 A. I didn't have them. That's not the correct
22 wording.

23 Q. Word it for me, then.

24 A. I had the access, which was — I had access to this
25 kind of bitcoin, but I was not the only one that had

Mr. Tiberiu Danet - Cross

1 access to it.

2 Q. Bitcoin was your bitcoin, correct?

3 A. No.

4 Q. Well, you said in your plea that you had access
5 through your computer, through an encrypted partition of
6 100 the 200 bitcoins, correct?

7 A. Yes.

8 Q. Okay. And this is — I mean, that's your nest egg,
9 right? That's what you put together. That's what you
10 have left over from this conspiracy?

11 A. No. That's not what I have left over.

12 Q. You have more than that?

13 A. A lot more people have access to that bitcoin.

14 Q. Okay.

15 A. Or at least one.

16 Q. Okay. Well, that would be your brother, right?

17 A. No. That would be Nicolescu.

18 Q. Well, if Mr. Nicolescu had access to it, then that
19 would be the only other person, just you and
20 Mr. Nicolescu?

21 A. As far as I know. I have no way of knowing who he
22 gave access to.

23 Q. Okay. But you didn't give access to anybody?

24 A. No.

25 Q. And the Government gave you a computer and — out in

Mr. Tiberiu Danet - Cross

1 the prison where you were staying — and let you work on
2 it to try to access the bitcoin, correct, among other
3 things?

4 A. Yeah, to try to access the container, not so much
5 the bitcoin.

6 Q. Okay. And this is a password that you had at one
7 point, right?

8 A. It is actually a combination of six passwords.

9 Q. All right. Well, you had that at one time,
10 right?

11 A. Yes. I did have it at one time.

12 Q. Okay. But now that you have to turn it over to the
13 Government, you can't find it. You can't figure out what
14 it is?

15 MR. BROWN: Objection.

16 THE COURT: Overruled. Is that correct,
17 sir?

18 THE WITNESS: I have to — so the six
19 passwords total up to a hundred characters.

20 BY MR. GOLDBERG:

21 Q. Okay.

22 A. It is not like "I love you mom" password, "Robert
23 12," you know.

24 Q. Listen, criminals use long passwords?

25 A. Exactly.

Mr. Tiberiu Danet - Cross

1 Q. And you were a criminal for eight, nine years?

2 A. Yes.

3 Q. With a couple vacations in between?

4 A. Yes.

5 Q. And you use passwords everyday to get into whatever
6 computer you needed to get into, right?

7 A. No. The reason I remember my password —

8 Q. Either you did or didn't. The question is: You
9 used computers, everyday password protected when you were
10 working as a criminal, right?

11 A. Which computers do you mean?

12 Q. You used a computer everyday to commit criminal
13 activity, right?

14 A. Most of the passwords I used during —

15 Q. Excuse me. The answer to that is yes or
16 no.

17 A. No. Most of the passwords are stored in files.
18 They are not stored —

19 Q. So you used a computer for criminal activity
20 most days when you were active in the conspiracy,
21 correct?

22 A. Yes.

23 Q. And every time you used the computer, you had to
24 access passwords, correct?

25 A. Yes.

Mr. Tiberiu Danet - Cross

1 Q. All right. And those passwords are important
2 because if you don't have them, you can't do your
3 criminal activity, right?

4 A. Yes.

5 Q. And you had since — you had over a year and-a-half
6 at this point — well, you had about nine months
7 working with that computer to try to find the password,
8 correct?

9 A. Um —

10 Q. Let's back up.

11 You proffered, you gave a statement to the
12 United States in July of 2018, right?

13 A. Yes.

14 Q. Okay. So — and did you have the computer before
15 you proffered to the Government?

16 A. No.

17 Q. And part of that proffer was to give that
18 information, right —

19 A. Yes.

20 Q. — to help them with their case?

21 A. Yes.

22 Q. And if it was truthful and if the Government found
23 that you were believable, you would get credit for it,
24 right?

25 A. Yes.

Mr. Tiberiu Danet - Cross

1 Q. And part of that agreement also required you to give
2 passwords, right?

3 A. Yes.

4 Q. So the Government —

5 A. Which I did.

6 Q. — so the Government at that point made sure that
7 you got a computer, so that you could find the passwords,
8 so they could get the bitcoin and any other —

9 MR. BROWN: Objection.

10 THE COURT: Sustained.

11 BY MR. GOLDBERG:

12 Q. Did the Government give you a computer at that
13 point?

14 A. No. It was only after a couple of months when they
15 had tried what I had provided.

16 Q. Okay. So you gave them — verbally, you gave them
17 passwords, right?

18 A. Yes. The reason it took that long was —

19 Q. Well, here. Just answer my questions yes or no.
20 Verbally, you gave them passwords, right?

21 A. Yes.

22 Q. All right. And Agent Macfarlane wrote them
23 down?

24 A. Yes. It was not just one password because I
25 couldn't remember certain characters or symbols or

Mr. Tiberiu Danet - Cross

1 combination of passwords. You had to try multiple
2 combinations to be able to see which one worked, which
3 was a process that needed time.

4 MR. GOLDBERG: May I approach, your Honor?

5 THE COURT: You may.

6 BY MR. GOLDBERG:

7 Q. Do you remember the exact passwords you gave to the
8 Government during the proffer?

9 A. After another — I remember, yeah, part of them.

10 Q. Okay. Would it help you if I showed you the notes
11 from that proffer?

12 A. Yeah.

13 Q. Okay. So I am showing you — I will have this
14 marked as Defendant's Exhibit M.

15 Do these look like passwords you turned over
16 to the Government?

17 A. Yes.

18 Q. And what day did that occur?

19 A. That — July something, July in 2018.

20 Q. Okay. That was the first meeting?

21 A. Yes.

22 Q. Okay. And down at the bottom, you see —

23 MR. BROWN: Your Honor, could we see what
24 Exhibit M is?

25 THE COURT: Certainly.

Mr. Tiberiu Danet - Cross

1 (Pause.)

2 BY MR. GOLDBERG:

3 Q. Down at the bottom, there is a notation that says
4 "bitcoin" —

5 MR. BROWN: Objection.

6 Q. — correct?

7 MR. BROWN: Objection.

8 THE COURT: Sustained.

9 BY MR. GOLDBERG:

10 Q. Did you give them a bitcoin password?

11 A. Define "bitcoin password."

12 Q. Did you give them a user name and password to get
13 them into the LUKS partition —

14 MR. BROWN: Objection.

15 Q. — to obtain the bitcoin?

16 MR. BROWN: Objection.

17 THE COURT: Sustained.

18 BY MR. GOLDBERG:

19 Q. What did you say to them? What did you give
20 them?

21 A. Multiple passwords that helped get in all the
22 encrypted containers that I had, which were layered. So
23 you needed several passwords to get in the first one and
24 so on.

25 Q. And did the password as far as you know or the

Mr. Tiberiu Danet - Cross

1 partial password that you gave them for the bitcoin
2 container, did it open the container?

3 A. No. That was inside another container that couldn't
4 be opened.

5 Q. Okay. And there were other containers within your
6 laptop that also contained partitions that couldn't be
7 opened as well, correct?

8 MR. BROWN: Objection.

9 THE COURT: Overruled. Do you know, sir?

10 A. Can you —

11 Q. Yeah.

12 A. Repeat the question.

13 Q. Once you gave all the passwords to the Government,
14 they used it on your devices, correct, as far as you
15 know?

16 A. Yes.

17 Q. And they were only able to access one container,
18 right?

19 A. Yes.

20 Q. And that container contained personal information,
21 personal pictures and videos?

22 A. No.

23 Q. It contained information regarding this —

24 A. Yes.

25 Q. — conspiracy?

Mr. Tiberiu Danet - Cross

1 A. Yes.

2 Q. Okay. But they were not able to access any of the
3 other material on your computer, correct?

4 THE COURT: I am going to sustain the
5 objection now.

6 BY MR. GOLDBERG:

7 Q. Do you know what happened when they tried to use
8 your passwords?

9 MR. BROWN: Objection.

10 THE COURT: Sustained.

11 BY MR. GOLDBERG:

12 Q. You — up until July of 2018, you had not sat down
13 with the Government to talk to them about this case,
14 correct?

15 A. Yes.

16 Q. And then when you did sit down with them, you were
17 in a room with your lawyer, with one or more of the
18 gentlemen sitting at this table, Mr. Macfarlane,
19 Agent Macfarlane, right?

20 A. Yes.

21 Q. Anyone else?

22 A. Agent Stacy Lough, L-o-u-g-h.

23 Q. And you said that that meeting occurred at the FBI
24 offices, correct?

25 A. Yes.

Mr. Tiberiu Danet - Cross

1 Q. And that lasted for how many hours?

2 A. The first one lasted probably six hours.

3 Q. Six hours. And the agents were taking notes during
4 the proffer, correct?

5 A. Yes.

6 Q. And you met with them later as well in the same kind
7 of circumstances?

8 A. Yes.

9 Q. All right. When was that?

10 A. I met two times again, the same office, then another
11 time here in the courthouse. I don't remember the dates,
12 but the ones in the FBI office were between July and
13 November of 2018.

14 Q. So twice between July and November?

15 A. No. I think it was four times.

16 Q. Four times?

17 A. Yeah.

18 Q. Okay. And one of the things that they were
19 interested in during that first six-hour meeting and the
20 meetings thereafter were the different monikers, the
21 different names of individuals engaged in the conspiracy,
22 correct?

23 A. Yes.

24 Q. In fact, they brought up the monikers pretty early
25 in the proffer. Would I be correct?

Mr. Tiberiu Danet - Cross

1 MR. BROWN: Objection.

2 THE COURT: Sustained.

3 BY MR. GOLDBERG:

4 Q. But they wanted to know monikers, right?

5 A. Yes.

6 Q. Okay. So you identified the moniker for Catalin
7 Dima, right?

8 A. Yes.

9 Q. You identified the moniker for Valentin Dima?

10 A. Danet.

11 Q. Okay.

12 MR. GOLDBERG: May I approach, your Honor?

13 THE COURT: Yes.

14 BY MR. GOLDBERG:

15 Q. I will show you what I will have marked as Defense
16 Exhibit N. Do you see the names?

17 A. Yes. I only mentioned —

18 THE COURT: One moment.

19 MR. BROWN: Objection. First of all, could
20 we see —

21 THE COURT: Show him the document.

22 MR. BROWN: We are going to object to
23 marking this exhibit.

24 THE COURT: Well, it can be marked.

25 MR. BROWN: But the objection is to the use

Mr. Tiberiu Danet - Cross

1 of it.

2 THE COURT: Side bar.

3 (Side bar held on the record.)

4 THE COURT: May I see it?

5 MR. O'SHEA: Judge, I don't have an
6 argument, so I am going to sit down. Okay?

7 THE COURT: Sure. Is this his proffer?

8 MR. BROWN: That's the first proffer.

9 MR. GOLDBERG: That's his proffer, his
10 statement.

11 THE COURT: You need to be closer.

12 MR. GOLDBERG: This is his first proffer
13 that occurred in July, I think, 2018.

14 THE COURT: What are you doing with this?

15 MR. GOLDBERG: I wish to point out with this
16 witness that he identified monikers and people during
17 that meeting. He may have misled the Government
18 regarding the moniker involving his brother, and he did
19 not identify Master Fraud or by a moniker in that
20 meeting.

21 THE COURT: You can use this for
22 impeachment, but you are not — you are not using it
23 appropriately at this point.

24 MR. GOLDBERG: But for the next question, I
25 probably —

Mr. Tiberiu Danet - Cross

1 THE COURT: But right now you haven't.

2 MR. GOLDBERG: Okay. All right. Thank
3 you.

4 THE COURT: I apologize. Was that your
5 objection?

6 MR. BROWN: Yes, your Honor.

7 (Side bar concluded.)

8 BY MR. GOLDBERG:

9 Q. When you were asked about various monikers, you
10 identified Catalin Dima, correct?

11 A. Yes.

12 Q. And I asked you about Valentin Dima, and you said
13 that was Valentin Danet?

14 A. I thought you were — I didn't know what you were
15 talking about.

16 Q. Well, did you identify your brother Valentin Danet
17 during that proffer?

18 A. Yes.

19 Q. What about a moniker for Mr. Metei Marius,
20 M-a-r-i-u-s?

21 A. I did not know that name.

22 Q. You didn't?

23 A. No.

24 Q. What about the name Master Fraud, did you associate
25 the name Master Fraud or MF with Mr. Nicolescu during

Mr. Tiberiu Danet - Cross

1 that six-hour proffer?

2 A. Yes.

3 Q. And if you did that, then, it would be reasonable to
4 assume that Agent Macfarlane wrote that —

5 MR. BROWN: Objection.

6 THE COURT: Sustained.

7 BY MR. GOLDBERG:

8 Q. Was Agent Macfarlane taking notes while you were
9 talking?

10 A. Yes.

11 Q. If I showed you —

12 MR. BROWN: Objection.

13 BY MR. GOLDBERG:

14 Q. If I showed you the notes taken at that proffer
15 meeting, can you point out in the notes that you
16 identified Nicolescu as Master Fraud?

17 THE COURT: Sustained.

18 BY MR. GOLDBERG:

19 Q. Have you had a chance to go through your statement
20 that was recorded by Agent Macfarlane in preparation for
21 Court?

22 A. No.

23 Q. So you haven't seen the notes at all?

24 A. No.

25 Q. But you are saying that you identified Nicolescu as

Mr. Tiberiu Danet - Cross

1 Master Fraud at that meeting for sure?

2 A. Yes.

3 Q. And there would be no reason that you could think of
4 why Agent Macfarlane wouldn't put that down?

5 MR. BROWN: Objection.

6 THE COURT: Sustained, sustained. Folks,
7 disregard that last question.

8 BY MR. GOLDBERG:

9 Q. Did you identify anybody else by moniker during the
10 meeting?

11 A. Yes.

12 Q. Who else?

13 A. Ionut Flueraș.

14 Q. Did you give a moniker for him?

15 A. Yes. He had one ID on Yahoo and another one on one
16 of the criminal accounts, something starting with W.

17 Q. Do you remember coming in here and pleading guilty,
18 right?

19 A. Yes.

20 Q. And you signed a long plea agreement that you said
21 you looked over very carefully?

22 A. Yes.

23 Q. And that plea agreement contained a number of
24 factual allegations that you had to sign off on?

25 A. Yes.

Mr. Tiberiu Danet - Cross

1 Q. You went over each of those paragraphs with your
2 attorney, correct?

3 A. Yes.

4 Q. Did you compare them with the indictment? In other
5 words, did you look at the agreement you were asked to
6 sign and the indictment and see which paragraphs matched
7 which paragraphs?

8 A. Not really. I hadn't identified which paragraph
9 matched.

10 Q. So if the factual basis that you signed off on
11 matched the language of the indictment, you — that would
12 be a surprise to you?

13 MR. BROWN: Objection.

14 THE COURT: Sustained.

15 BY MR. GOLDBERG:

16 Q. Now, you talked about what you were getting out of
17 the plea agreement, and you were not so sure about what
18 you were actually facing —

19 MR. BROWN: Objection.

20 Q. — yesterday during your testimony, right? Am I
21 remembering that correctly?

22 THE COURT: Overruled. Is that correct,
23 sir?

24 THE WITNESS: Can you repeat that?

25 MR. GOLDBERG: Yes.

Mr. Tiberiu Danet - Cross

1 BY MR. GOLDBERG:

2 Q. So you had a year-and-a-half before you started
3 to cooperate, to talk about what kind of sentence
4 you could look at if you are convicted in this case,
5 right?

6 A. Yes, but I was not really getting anywhere with my
7 attorney.

8 Q. Wait. You had two attorneys?

9 A. That —

10 Q. You had two attorneys, right?

11 A. I had two attorneys prior to — yeah. I hired a
12 second attorney.

13 Q. And you were not getting anywhere with either one of
14 them?

15 MR. BROWN: Objection.

16 THE COURT: Sustained.

17 BY MR. GOLDBERG:

18 Q. Well, listen, luckily it is right in your plea
19 agreement what you were looking at?

20 MR. GOLDBERG: And I have had this marked as
21 Defendant's Exhibit F, your Honor.

22 THE COURT: Did you say F?

23 MR. GOLDBERG: F, the plea agreement.

24 BY MR. GOLDBERG:

25 Q. So do you recognize Defendant's Exhibit F?

Mr. Tiberiu Danet - Cross

1 A. Yes. It is my plea agreement.

2 Q. Okay. And those are your initials at the
3 bottom?

4 A. Yes.

5 Q. And did you initial each page?

6 A. Yes.

7 Q. And did you go over this with both your attorneys?

8 A. Yes.

9 Q. Okay. And starting on page 9, there are sections
10 that talk about the Federal Sentencing Guidelines,
11 correct?

12 A. Yes.

13 Q. Okay. And I know you didn't just sign this and not
14 ask what this all meant, right?

15 A. Yes.

16 Q. Okay. And those guideline calculations go on to
17 page 10 as well, correct?

18 A. Yes.

19 Q. Okay. And does it give a number that relates to
20 your total offense level before acceptance of
21 responsibility?

22 A. Yes.

23 Q. Okay. What's that number?

24 A. 35.

25 Q. Now, did you talk to your attorneys about what level

Mr. Tiberiu Danet - Cross

1 35 means?

2 A. Yes, I did.

3 Q. Okay. And what was your understanding of the
4 sentencing range for a level 35?

5 A. This being 11(c) (1) (C) —

6 Q. No.

7 A. — plea.

8 Q. Without the (c) (1) (C.)?

9 A. But it is 11(c) (1) (C) with that guideline
10 calculation. That's what I understood.

11 Q. Your 11(c) (1) (C) means you agreed to a range.

12 A. Yes.

13 Q. Without the range, what would your guideline level
14 be?

15 A. But I did not sign a plea without the range.

16 Q. You are right. You signed a plea with a range, but
17 you also have an offense level, correct?

18 A. Yes.

19 Q. And do you think if you wouldn't have pled guilty
20 and signed this agreement and agreed to testify you would
21 be looking at a (c) (1) (C) sentence or something closer to
22 the guideline sentence?

23 MR. BROWN: Objection, your Honor.

24 THE COURT: Sustained. Rephrase your
25 question.

Mr. Tiberiu Danet - Cross

1 BY MR. GOLDBERG:

2 Q. You knew to get the (c) (1) (C) range, you had to
3 cooperate with the Government, right?

4 A. I did not know that before cooperating.

5 Q. Okay. But you know it now, right?

6 A. Yes. Once I got the plea agreement, obviously, I
7 read it and know the terms of it.

8 Q. Right. And the 35 is the offense level you
9 discussed, or you knew — you knew what that 35 meant. I
10 will back up and start over.

11 You knew what offense level 35 meant,
12 correct?

13 A. Yes, but I did not know I was at a 35 until
14 receiving the plea agreement.

15 Q. Okay. But then, you got the plea agreement, and you
16 saw that's where you would be, but you made a deal and
17 you got lower, right?

18 A. No. I received the plea agreement of a range of
19 9 to 12 with a level 35. It is in the same plea
20 agreement.

21 Q. So for the year-and-a-half you had one or two
22 lawyers, they never told you —

23 MR. BROWN: Objection, your Honor.

24 THE COURT: Sustained.

25

Mr. Tiberiu Danet - Cross

1 BY MR. GOLDBERG:

2 Q. You had to have discussed what sentencing you were
3 facing.

4 A. You mean before getting the plea agreement?

5 Q. Of course.

6 A. Yeah. I know the statutory maximum, which is
7 the maximum, but when you say what you are facing, I
8 usually —

9 Q. Well, what's the statutory maximum?

10 A. I believe it is 27 years or something like that.

11 Q. Okay. And does the aggravated identity theft
12 counts, do they add anything to that?

13 A. Yes. If you are found guilty, yeah.

14 Q. What do they add?

15 A. Two years each.

16 Q. And how many are there?

17 A. Maximum of two years. Yes, five.

18 Q. So it is 37 years?

19 A. Right.

20 Q. So you knew it very well. We didn't have to go
21 through all that.

22 You were looking at 37 years?

23 MR. BROWN: Objection.

24 THE COURT: Sustained.

25

Mr. Tiberiu Danet - Cross

1 BY MR. GOLDBERG:

2 Q. You were looking up to 37 years?

3 A. No. The statutory maximum, that's the absolute
4 maximum somebody can get.

5 Q. That's what I am saying.

6 A. It is not one in the same thing looking at —

7 Q. Before you signed the plea agreement, you had a
8 maximum sentence of 37 years, correct?

9 A. Yeah. But it could be as low as five years. There
10 is other things involved than just the statutory maximum.
11 That doesn't decide your sentence.

12 Q. Right. The Guidelines do, and you went the over
13 those with your attorneys, too, right?

14 A. Yes.

15 Q. You saw this book, right?

16 A. Yes.

17 Q. Okay. You saw this table, correct?

18 A. Yes.

19 Q. Okay. What does it say for level 35?

20 A. It says 168 to 210. I don't understand the
21 relevance to my plea agreement, though.

22 Q. It says 168 months to 210 months, correct?

23 A. Yes.

24 Q. And that's before you add in the aggravated identity
25 theft count?

Mr. Tiberiu Danet - Cross

1 MR. BROWN: Objection.

2 Q. Correct?

3 THE COURT: Sustained.

4 BY MR. GOLDBERG:

5 Q. You went over all that with your attorneys before
6 you signed the plea agreement, correct?

7 A. You are forgetting to mention the 3 points for
8 acceptance of responsibility and other things, that
9 this came in the same plea agreement with the binding
10 range.

11 Q. Okay. I understand that you know all about the
12 Sentencing Guidelines, and I understand you know there is
13 a three-point reduction.

14 So you have to know that if you went to
15 trial, that you would face a sentence based close to the
16 range I just showed you, correct?

17 MR. BROWN: Objection.

18 THE COURT: Overruled. Do you know, sir?

19 THE WITNESS: I expected to get more than 12
20 years if I went to trial, yes.

21 BY MR. GOLDBERG:

22 Q. Right. You expected to get somewhere in the range
23 that I just showed you?

24 A. Yes.

25 Q. Okay. You also signed a cooperation addendum to

Mr. Tiberiu Danet - Cross

1 your plea agreement, correct?

2 A. Yes.

3 Q. And that's been marked as Exhibit G?

4 MR. BROWN: Yeah.

5 MR. GOLDBERG: Okay.

6 BY MR. GOLDBERG:

7 Q. What was your understanding of what the cooperation
8 addendum could do for you?

9 A. Honestly, I was — I have seen addendums like this
10 and usually mention points and mine didn't, so I was
11 pretty upset about that.

12 Q. Did it mention anything about other people in other
13 countries? You are welcome to look at it.

14 A. It did. I was not the one.

15 Q. Well, you signed it. You signed that agreement,
16 correct?

17 A. Yes, yes.

18 Q. You read it before you signed it?

19 A. Yes, I did.

20 Q. You went over it with your lawyers?

21 A. Yes.

22 Q. You stood in this courtroom and acknowledged your
23 signature before this Court?

24 A. Yes.

25 Q. Okay. What was your understanding of what you were

Mr. Tiberiu Danet - Cross

1 getting from the cooperation addendum?

2 A. I was not promised anything, and I didn't have an
3 understanding that I would be getting anything.

4 Q. Okay. Well, what were you obligated to do regarding
5 your cooperation addendum?

6 A. To cooperate fully with the Government.

7 Q. And give the names of people in Romania and
8 passwords?

9 A. Which I had already done, yes, in my proffer
10 meeting.

11 Q. You were supposed to give passwords and anything
12 that the Government needed to decrypt your computers,
13 correct?

14 A. Yes.

15 Q. And they still haven't done that, have they?

16 A. Not to my understanding.

17 Q. Okay. You were supposed to identify any unindicted
18 members of the Bayrob Group, and if they choose to
19 cooperate, they would get credit, right.

20 A. Which I had already done in my first proffer
21 meeting.

22 Q. Okay. But would you get credit if the other members
23 of the Bayrob Group who were unindicted cooperated? Was
24 that your understanding?

25 A. No. My understanding — because that addendum

Mr. Tiberiu Danet - Cross

1 doesn't mention any points for cooperation. I don't have
2 any understanding that I would be getting anything more
3 than my nine to twelve-year plea.

4 Q. Would you be closer to nine or twelve?

5 MR. BROWN: Objection.

6 Q. If you sent people in from Romania to talk to the
7 Government?

8 THE COURT: Sustained.

9 BY MR. GOLDBERG:

10 Q. You have indicated that you had a personal use
11 Jabber server at your home, correct?

12 A. Excuse me. Yes.

13 Q. And was that contained — was that a separate
14 machine, or was it contained within a desktop or a laptop
15 that was in your apartment?

16 A. It was — yeah. It was contained in sort of a
17 desktop computer, a smaller one.

18 Q. Okay. Was there a brand name on it?

19 A. It was an Intel computer.

20 Q. It was an Intel computer?

21 A. Yes.

22 Q. Okay. So have you seen that Intel computer that
23 contained the Jabber server since your arrest?

24 A. No.

25 Q. Was anything else on the Intel computer besides a

Mr. Tiberiu Danet - Cross

1 Jabber server?

2 A. Yes. There were a lot of things.

3 Q. And the Jabber server, was it a software package?

4 Did you load it on to the computer?

5 A. Yes.

6 Q. And I assume since it was at your house, that you
7 were the system administrator for that Jabber server?

8 A. Yes.

9 Q. Which means that you could — you have full access
10 to the data stored in the conversations relating to any
11 Jabber chats, right?

12 MR. BROWN: Objection.

13 THE COURT: Sustained.

14 BY MR. GOLDBERG:

15 Q. Well, you had — you were system administer, and you
16 could access the server, correct?

17 A. Yes.

18 Q. The Jabber server.

19 And you could access the sign-in
20 credentials of any person signing on to that Jabber
21 server, correct?

22 A. Yes.

23 Q. And that Jabber server could be accessed by any
24 device in the world as long as that person who was
25 accessing it had the sign-in credentials and the web

Mr. Tiberiu Danet - Cross

1 address, correct?

2 MR. BROWN: Objection.

3 THE COURT: One moment. Overruled. Can you
4 answer that, sir?

5 THE WITNESS: Yes.

6 BY MR. GOLDBERG:

7 Q. Could — if you had the Jabber — you used to make
8 mobile chats on a server, correct, from a SmartPhone?

9 A. Yes.

10 Q. And is that an application that you download and
11 put on your SmartPhone like I would download any
12 application?

13 A. Yes.

14 Q. And what kind of SmartPhone did you use?

15 A. I once had a Samsung. Then I changed it for another
16 one.

17 Q. Okay. And as long as you have got that application
18 and the application knows where the server is, you can
19 sign in to that Jabber server, correct?

20 A. Yes.

21 Q. And as long as you had the user ID and the password,
22 you could sign in as that person, correct?

23 A. Yes.

24 Q. And in fact, more than one person can sign on
25 under the same user ID and password at the same time,

Mr. Tiberiu Danet - Cross

1 correct?

2 A. Not really. That's why we had different accounts
3 for the mobile and the computer.

4 Q. Okay. So — but all right.

5 So different accounts for the mobile and the
6 computer, but the same individual could sign on from two
7 different devices at once?

8 A. On to the different accounts.

9 Q. Okay. But you can't have two people on the same
10 account?

11 A. It is either you can't have more or doesn't work
12 properly. I don't know which one it isn't but —

13 Q. So you are not sure?

14 A. I am not sure, and it doesn't work properly or might
15 not even be possible.

16 Q. So let's say you had a Jabber account on your server
17 in the name of Michael and another one in the name of
18 O'Shea, let's say, two different people, right?

19 A. Yes.

20 MR. BROWN: Objection.

21 THE COURT: Let me hear the question.

22 BY MR. GOLDBERG:

23 Q. Is there anything to prevent me from signing on
24 as Michael on one device and as O'Shea on another
25 device?

Mr. Tiberiu Danet - Cross Cont'd

1 THE COURT: Overruled.

2 Q. At the same time?

3 A. No.

4 MR. GOLDBERG: Thank you. Nothing further.

5 THE COURT: Cross examination, Mr. O'Shea?

6 MR. O'SHEA: Thank you.

7 CROSS EXAMINATION CONTINUED

8 BY MR. O'SHEA:

9 Q. Good morning, sir.

10 A. Good morning.

11 Q. If I ask you a question and you are not — and you
12 give me a response and I start my next before you are
13 done with your response, will you tell me?

14 A. Okay.

15 Q. Okay. I don't want to cut you off. Okay?

16 A. All right.

17 Q. All right. Now, let me take you back to September
18 28, 2016. You remember that day, do you not, sir?

19 A. Yes.

20 Q. What happened on that day?

21 A. I was arrested.

22 Q. Okay. Who was with you when you got arrested?

23 A. You mean at the moment?

24 Q. Yes, sir.

25 A. Nobody.

Mr. Tiberiu Danet - Cross Cont'd

1 Q. You were all by yourself?

2 A. Yes.

3 Q. Where were you?

4 A. In my apartment.

5 Q. Okay. And when did you become aware that other
6 people had been arrested?

7 A. Only hours later when I got to the offices of — it
8 is called the Court. It is kind of an FBI in Romania.

9 Q. Romanian National Police?

10 A. Yes, a special office.

11 Q. And when you got there, did you see other people
12 that had also been arrested?

13 A. There was a room full of people. Nobody was
14 handcuffed, so I didn't know if they were arrested or
15 not.

16 Q. Were you handcuffed?

17 A. No.

18 Q. Now, did you get a chance to talk to anybody else in
19 the room that day?

20 A. No.

21 Q. Did you recognize some of the people in the room
22 that day?

23 A. No.

24 Q. They were all strangers to you?

25 A. When I had gotten there, there were only two people

Mr. Tiberiu Danet - Cross Cont'd

1 I had never seen, yes.

2 Q. And since that day, have you seen any of the two
3 Defendants in this case?

4 A. Yes.

5 Q. Where did you see them?

6 A. In jail and in Romania and here.

7 Q. Did you see them in Romania?

8 A. You mean after I got arrested or before?

9 Q. After you got arrested.

10 A. Yes.

11 Q. Okay. Now, from what I am hearing you tell us, you
12 knew a lot of the people that were allegedly involved
13 with this organization, right, you yourself?

14 A. Actually, I knew very few of the people of all the
15 ones that I — that I knew existed, but I didn't know who
16 they were.

17 Q. And how many people do you think existed?

18 A. Maybe close to ten.

19 Q. And you would agree with me that probably all ten of
20 them knew you had gotten arrested, correct?

21 MR. BROWN: Objection.

22 THE COURT: Sustained.

23 BY MR. O'SHEA:

24 Q. Do you know if anybody else knew that you got
25 arrested other than yourself?

Mr. Tiberiu Danet - Cross Cont'd

1 MR. BROWN: Objection.

2 THE COURT: Sustained.

3 BY MR. O'SHEA:

4 Q. Did you ever have a conversation with anybody about
5 other people that got arrested?

6 MR. BROWN: Objection.

7 THE COURT: Sustained.

8 BY MR. O'SHEA:

9 Q. Do you have any specific formal computer skills,
10 training, sir?

11 A. Yeah. I did finish university.

12 Q. What university?

13 A. University of Bucharest.

14 Q. Okay. And what did you get your degree in? Do you
15 know what I mean by that?

16 A. It is — yeah. It was the faculty — it is called
17 mathematics and informatics, and that means computer
18 science.

19 Q. And did you get a degree in computer science?

20 A. Yes.

21 Q. All right. And when did you get that degree, what
22 year?

23 A. 2007.

24 Q. And did you ever have a legitimate job using those
25 skills?

Mr. Tiberiu Danet - Cross Cont'd

1 A. Yes.

2 Q. Which jobs?

3 A. Software developer part-time; also did the
4 internship with Google.

5 Q. Did you get paid?

6 A. Yes.

7 Q. Okay. Did you do that here in the United States or
8 over here?

9 A. The first time part-time over there and the other
10 one here in the United States.

11 Q. After you learned those skills, did you ever donate
12 your time to the Red Cross or any charity or anything
13 like that?

14 MR. BROWN: Objection.

15 THE COURT: Sustained.

16 BY MR. O'SHEA:

17 Q. Is it your testimony in front of this jury,
18 other than that short-lived job that you had, all you
19 utilized your skills for was to deceive and defraud
20 people?

21 A. No.

22 Q. My last question: What volunteer work did you do to
23 assist your fellow Romanians with your skills?

24 MR. BROWN: Objection.

25 THE COURT: Sustained.

Mr. Tiberiu Danet - Cross Cont'd

1 BY MR. O'SHEA:

2 Q. Now, just so I understand you, sir, other than those
3 two jobs that you talked about, all of your other
4 computer skills you dedicated to just things that
5 benefited you and/or your fraudulent activities. Am I
6 right?

7 MR. BROWN: Objection.

8 A. No. I had another job.

9 Q. So we have a third job?

10 A. Yes.

11 Q. What was that?

12 A. Software engineer again for a company.

13 Q. How long was that?

14 A. It was a couple of years, but I was working from
15 home.

16 Q. Okay. Let me rephrase my last questions:

17 Other than those three jobs, isn't it true
18 that all of your computer skills were utilized for your
19 personal needs or fraudulent activities?

20 MR. BROWN: Objection.

21 THE COURT: Overruled.

22 A. No. I had a lot of hobbies, too. I had been using
23 those. Not everything I do was related to this scheme.
24 I had other interests and hobbies relating to technical
25 stuff that had nothing to do with the criminal scheme.

Mr. Tiberiu Danet - Cross Cont'd

1 Q. But the hobbies were for you, right?

2 A. Yes.

3 Q. Okay. Now, let me ask you this, sir.

4 The money —

5 A. I just thought of something.

6 Q. Okay. You had a fourth job?

7 A. No. It is — I worked with a professor from the
8 university. I think you can find it online, wrote an
9 article and did some search about languages and the
10 similarities between languages by using computer science.

11 Then, when I was in college, it keeps coming
12 to me, when I was in college, I also volunteered to be
13 on the team of professors that are educating the high
14 school national team of Romania, and I did that several
15 times.

16 Q. For what?

17 A. For computer science, and I did that several times,
18 three years in a row if I am not mistaken.

19 Q. Okay. After you got your degree while you were in
20 college, like a lot of students, you are a part-time
21 teacher and helping. Other than that, after you got your
22 degree in those three jobs, your answer that you gave me
23 before still stands, right?

24 A. Yes. The answer that I gave you before still
25 stands.

Mr. Tiberiu Danet - Cross Cont'd

1 Q. Now, let's talk about the money that you made
2 defrauding people with your computer skills.

3 I think Mr. Goldberg asked you this, and I
4 just want to follow-up. Where is it, the money?

5 A. So a large chunk of it I gave to Nicolescu's
6 father.

7 Q. Was he a charity? Why did you give it to him?

8 A. I didn't actually give it. Nicolescu assured me it
9 was a good investment to give the money to his father,
10 and I personally know that he did the same. He gave
11 a lot of money to his father that he has never seen
12 back.

13 Q. And tell the ladies and gentlemen of the jury when
14 you called the Romanian authorities and told them about
15 the money you made so you could pay the income taxes.
16 When did you do that?

17 A. I actually paid quite a bit of income tax.

18 Q. I am talking about the money you made from your
19 illegal activities.

20 Are you telling us you called the Romanian
21 authorities, said "look, I am doing this illegal stuff.
22 I made money. I want to pay taxes on it."

23 Did you do that?

24 A. I was paying the tax on items I bought in
25 Romania.

Mr. Tiberiu Danet - Cross Cont'd

1 Q. That's sales tax. I am talking about income
2 tax.

3 A. I didn't pay income tax for this ones.

4 Q. And all the money you made from all the frauds, that
5 you told the Romanian authorities that you are going to
6 go ahead now that you have been caught, you are going to
7 go ahead and pay your income taxes on it.

8 When have you done that?

9 A. I haven't.

10 Q. I thought you were cooperating.

11 MR. BROWN: Objection.

12 THE COURT: Sustained.

13 MR. O'SHEA: Okay.

14 BY MR. O'SHEA:

15 Q. Now, you spent a long time preparing for your
16 testimony with these gentlemen to my left. Am I right,
17 sir?

18 A. No. I spent more time giving information about the
19 case than preparing for testimony.

20 Q. Okay. You are not going to tell the ladies and
21 gentlemen of the jury that the first time you saw those
22 exhibits that were up on your screen yesterday was in the
23 courtroom, right?

24 MR. BROWN: Objection.

25 THE COURT: Sustained.

Mr. Tiberiu Danet - Cross Cont'd

1 BY MR. O'SHEA:

2 Q. Did you see those exhibits you saw on your computer
3 screen for the first time yesterday, on the computer
4 screen, or had you seen them before?

5 A. I had seen them before shortly.

6 Q. Okay. And during that process when you saw
7 them before, things were pointed out for you, so you
8 would know what they looked like in the courtroom,
9 correct?

10 A. No.

11 MR. BROWN: Objection.

12 THE COURT: Sustained.

13 BY MR. O'SHEA:

14 Q. As part — did part of your criminal fraudulent
15 activity, sir, that you did on a regular basis with your
16 computer skills in Romania involve stealing user names
17 and passwords?

18 A. Yes.

19 Q. Why do you want to know what user name and passwords
20 are? Why?

21 A. For example, some of the accounts were sent, were
22 used to send e-mails.

23 Q. You want user name and passwords so you can go into
24 someone's account like a Yahoo or Google and use that
25 account for your benefit, right?

Mr. Tiberiu Danet - Cross Cont'd

1 MR. BROWN: Objection.

2 THE COURT: Overruled. You may answer that,
3 sir.

4 A. No. It was not like going personally into
5 somebody's account. Those accounts were part of a
6 database. They were just information, data.

7 Q. What value do user names have for you, the user
8 names and passwords, if you are not using them to get
9 into accounts?

10 A. You are using them to get into accounts in a
11 sense.

12 Q. Does Pidgin even require a user name and password?

13 A. Yes.

14 Q. Does Yahoo require a user name and password?

15 A. Yes.

16 Q. Does Jabber require a user name and password?

17 A. Yes. Jabber is just a protocol.

18 Q. Just so that I am clear, you never saw a specific
19 computer infected with anything from where you were,
20 right?

21 MR. BROWN: Objection.

22 THE COURT: Overruled. Can you answer?

23 A. I don't understand.

24 Q. Did you ever see a specific computer like this or a
25 computer over here, did you ever see yourself a specific

Mr. Tiberiu Danet - Cross Cont'd

1 computer anywhere in the United States infected?

2 A. Physically, no.

3 Q. What's a web history or a cookie? Tell the ladies
4 and gentlemen of the jury what those are.

5 A. The web history is the history of web pages accessed
6 by somebody.

7 Q. And how do cookies help that?

8 A. It is a strange question. They don't help. It is
9 something else.

10 Q. All right. What do they do? What do cookies
11 do?

12 A. They store information, for example, when you are
13 logged into a website. That way it knows when you are
14 coming back that you are the same person because that is
15 stored in a cookie.

16 Q. And the cookies are on your computer, right, the guy
17 that is logged in?

18 A. No. The cookies are on the person's computer that
19 is using the computer.

20 Q. So if I log into a Yahoo or Google account or any
21 website where I bought something, that website knows it
22 is the same computer because that website put cookies on
23 that computer, right?

24 A. Yes.

25 Q. And to the best of your understanding, it did it

Mr. Tiberiu Danet - Cross Cont'd

1 without permission, right?

2 A. Actually, I don't know the law in the United States,
3 but in the European Union, all the websites display a
4 wording about that.

5 Q. Okay. Now, can you put up Exhibit 1852? Do you
6 remember being shown this exhibit yesterday, sir?

7 A. Yes.

8 Q. Was this one of the exhibits they showed you before
9 you took the witness stand?

10 A. There were many e-mail tables containing e-mails
11 such as this.

12 So I can't remember if this was one of them
13 or not.

14 Q. Okay. Mr. Danet, do you remember seeing this
15 exhibit yesterday, sir?

16 A. Yes.

17 Q. Do you remember seeing it before you sat down on the
18 witness stand yesterday?

19 A. Not particularly.

20 Q. So what you are telling these folks here, for the
21 first time in your life when you saw this exhibit was
22 yesterday when it was on the screen?

23 A. No. I said I did not remember if I saw it before or
24 not. That was your question.

25 Q. Okay. All right. Now, what do you think this

Mr. Tiberiu Danet - Cross Cont'd

1 exhibit is?

2 A. It is a list of e-mails sent and probably received
3 by the account amightysa@gmail that I was using.

4 Q. Do you know where they are from, how they came
5 onto this exhibit, this information? Do you have any
6 idea?

7 A. Not particularly, but I can only suppose. I can
8 only —

9 Q. Okay. Now, the files that are referenced in some of
10 these communications, are they all encrypted?

11 A. Most of them are, but I don't know if all are
12 encrypted. I would have to check all the pages to see if
13 they are encrypted. Usually when they are encrypted,
14 they have a certain extension.

15 Q. Very well. Can you pull up Exhibit 367? Do you see
16 Exhibit 367?

17 A. Yes.

18 Q. Do you remember being shown this yesterday?

19 A. Yes.

20 Q. Same questions before you have sat down on that
21 witness stand yesterday, had you ever seen this document
22 before?

23 A. You mean all 538 pages of it? No.

24 Q. The document itself?

25 A. What — what do you mean by "seeing the document"?

Mr. Tiberiu Danet - Cross Cont'd

1 I have seen a lot of tables and documents. I haven't
2 checked page by page each page. There is a list of chat
3 messages, yes.

4 Q. Do you even know what this is?

5 A. It is a list of messages between me, I suppose, and
6 I would have to check the pages again and other people on
7 the Jabber account from my house.

8 Q. Do you even know how it was put together? Do you
9 have any idea?

10 A. Yes. I can see right at the top it is from the
11 server that was obtained from my house.

12 Q. Okay. How do you know that? How do you know how it
13 was put together?

14 A. Because it says in the beginning, asks you like file
15 name server .db, and that's a database.

16 Q. So it is your testimony, sir, that the — I think
17 there is 13 columns — that that was put together by the
18 server?

19 A. Yes.

20 Q. Okay. Showing you Exhibit 2203, prior to your
21 testimony yesterday, sir, before you sat down on
22 that witness stand, had you ever seen that document
23 before?

24 A. Yes. I believe this is part of the discovery.

25 Q. Okay. And this was a document that the Government

Mr. Tiberiu Danet - Cross Cont'd

1 showed you before you sat down, right?

2 A. It was part of the discovery. All the Defendants
3 seen it, yes.

4 Q. Here is my question to you, Mr. Danet. Let's not
5 get tricky. All right?

6 MR. BROWN: Objection.

7 THE COURT: Sustained.

8 BY MR. O'SHEA:

9 Q. Did you see this document marked as Exhibit 2203
10 when you met with the United States Attorneys prior to
11 your testimony yesterday, sir? Yes or no.

12 A. I have seen so many documents that it is hard for me
13 to say I seen this one. You can say yes, I probably seen
14 it.

15 Q. In your entire life, sir, have you ever had to give
16 an oath before for anything?

17 A. I don't remember. Probably not.

18 Q. Okay. Do you know that the oath that you took
19 here in this case requires you to be unconditionally
20 honest?

21 A. Yes.

22 Q. Do you even remember what the words of the oath
23 were, sir?

24 MR. BROWN: Objection.

25 THE COURT: Sustained.

Mr. Tiberiu Danet - Redirect

1 MR. O'SHEA: Nothing further, your Honor.

2 THE COURT: Any redirect?

3 MR. BROWN: Very briefly. Thank you, your
4 Honor.

5 REDIRECT EXAMINATION

6 BY MR. BROWN:

7 Q. Do you recall testifying with Mr. Goldberg about a
8 root account, user name and password?

9 A. Yes.

10 Q. Do you know who had the root account, user name and
11 password?

12 A. Like I said before yesterday, a couple of people
13 probably, four that I knew of.

14 Q. And who were those four?

15 A. I think I mentioned yesterday, Nicolescu, me,
16 Miclaus sometimes, and Linx.

17 Q. And do you recall on Mr. O'Shea's cross examination
18 he asked you if you had ever physically seen an infected
19 computer in the U.S.?

20 A. No.

21 Q. How did you know there were computers infected with
22 Bayrob Trojan in the United States?

23 MR. O'SHEA: Objection.

24 THE COURT: Overruled.

25 A. Excuse me. Because it showed whenever there was an

Mr. Tiberiu Danet - Redirect

1 investigated computer, you could see its location based
2 on its IP.

3 Q. And where would you see that?

4 A. There were services online. You put in an IP and
5 tells you where it is from.

6 Q. But where would you see where the infected computer
7 was talking to? Was that on the command and control?

8 A. Yes. It was in the list yesterday shown yesterday.
9 There was like — shown how every computer had a column
10 of state, city.

11 Q. Would it show up in the data bases of the command
12 and control servers?

13 A. Yes. It was part of the Trojan.

14 Q. Did it then become part of the Trojan, part of the
15 botnet?

16 MR. GOLDBERG: Objection.

17 THE COURT: Sustained.

18 BY MR. BROWN:

19 Q. Did the infected computer become part of the Bayrob
20 botnet?

21 A. Yes. That's — the botnet compromises the infected
22 computers.

23 MR. BROWN: Thank you. Nothing further,
24 your Honor.

25 THE COURT: Based on those questions,

Mr. Tiberiu Danet - Recross

1 Mr. Goldberg?

2 MR. GOLDBERG: Thank you.

3 RECROSS EXAMINATION

4 BY MR. GOLDBERG:

5 Q. The root account, you said four people had it. You
6 said your brother didn't have the root account log-in
7 password?

8 A. Like I said, I don't know if towards the end; I
9 know Miclaus didn't have it. So it just depends on
10 time.

11 Q. Okay. So you don't know whether your brother had it
12 or not?

13 A. Yes. I don't know.

14 Q. Okay.

15 A. I don't know if a lot of people had it, too.

16 Q. But your brother may have had it?

17 A. Yes, may have had.

18 Q. And you mentioned — there is a name on Exhibit
19 2203, which you were referring to with a root account, it
20 is L-i-n-x. Is that short for something?

21 A. No. I don't know.

22 Q. Do you know who that is?

23 A. Yes. It is Dima.

24 Q. And have you ever met him?

25 A. Once.

Mr. Tiberiu Danet - Recross

1 Q. And you are saying that he had it, definitely had
2 the password and log-in?

3 A. At a certain point, yes.

4 Q. And that's in addition to the other three or four
5 people, or was he included?

6 A. He is included in the three or four people.

7 Q. But your brother is not?

8 A. Yes. I don't know if he is or isn't.

9 Q. Well, you didn't mention your brother's name
10 yesterday as one of the people.

11 A. No, I hadn't.

12 Q. But today you are saying he may have had the
13 password?

14 A. Yesterday I gave a list of the people that I knew
15 had the password.

16 Q. Right. And today you said your brother had it,
17 too?

18 A. Yes, may have had. Again, there are people that
19 have probably had it, and I don't even know their names
20 or nicknames or anything.

21 Q. There could be an unlimited number of people that
22 had the passwords and log-ins, correct?

23 A. I wouldn't say unlimited, but, yes.

24 Q. Fifty, right?

25 MR. BROWN: Object.

Mr. Tiberiu Danet - Recross

1 A. 50, no.

2 Q. All right. So how many?

3 A. As many as Miclaus knew.

4 Q. Or you, you had them, right?

5 A. Yes.

6 Q. And you could have given them to somebody,
7 right?

8 A. I could have, yes.

9 Q. And if your brother had them, he could have given
10 them to somebody.

11 A. Yes.

12 Q. And everybody else whose name is on here, not just
13 Mr. Nicolescu?

14 A. Yes.

15 Q. I know that's what you want to say because that's
16 what your job is here.

17 MR. BROWN: Objection.

18 THE COURT: Sustained. Folks, disregard the
19 last statement.

20 BY MR. GOLDBERG:

21 Q. But anybody could have given these passwords to
22 anybody if they wanted to, right?

23 MR. BROWN: Objection.

24 A. Yes, as long as they had somebody involved in the
25 scheme, as long as they wanted someone else to be

Mr. Tiberiu Danet - Recross Cont'd

1 involved in the scheme.

2 MR. GOLDBERG: Okay. Thank you.

3 THE COURT: Recross, Mr. O'Shea?

4 RECROSS EXAMINATION CONTINUED

5 BY MR. O'SHEA:

6 Q. As you sit here today, sir, at 11:37 in Cleveland,
7 Ohio, can you name a single computer in the United States
8 that was infected by this so-called virus, a single
9 computer by name, city, street, address, anything?

10 A. What do you mean name of a computer? Computer
11 doesn't have a name. How am I going to name a
12 computer?

13 Q. Name, address, a person who owned it. As you sit
14 there right now without getting help from any
15 demonstrative exhibits or charts, as you sit there from
16 your own memory, can you name one?

17 A. Obviously not.

18 MR. O'SHEA: Thank you. Nothing further.

19 MR. BROWN: Nothing further.

20 THE COURT: Any redirect?

21 MR. BROWN: No.

22 THE COURT: Folks, we are going to take our
23 luncheon recess, and I know it is a little bit early, but
24 please be downstairs at 12:45. We will call for you at
25 that time. Remember the admonitions, folks. All rise

Mr. Tiberiu Danet - Recross Cont'd

1 for the jury.

2 (Jury out.)

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Mr. Vaduva - Direct

1 THE COURT: We are in recess folks.
2 (Luncheon recess.)

3 - - - - -
4
5
6
7
8
9

10 AFTERNOON SESSION

11 THE COURT: Please be seated. Please call
12 your next witness.

13 MR. LEVINE: The United States of America
14 calls Bogdan Vaduva.

15 THE COURT: Please step up to the podium,
16 sir. And please raise your right hand.

17 BOGDAN D. VADUVA
18 called as a witness by and on behalf of the Government,
19 being first duly sworn, was examined and testified
20 as follows:

21 DIRECT EXAMINATION

22 BY MR. LEVINE:

23 Q. Good afternoon.

24 A. Good afternoon.

25 Q. Mr. Vaduva, could you please state and spell your

Mr. Vaduva - Direct

1 last name for the court reporter.

2 A. Vaduva Bogdan Daniel and V-a-d-u-v-a, B-o-g-d-a-n,
3 and Daniel is like in the United States, D-a-n-i-e-l.

4 Q. Okay. So is Vaduva your family name?

5 A. Yes. Vaduva is my family name.

6 Q. And your first name or given name?

7 A. Would be Bogdan and Daniel my middle one. In
8 Romania, we start with the family name.

9 Q. Okay. And Mr. Vaduva, were you employed by the
10 Romanian National Police or the RNP at the time the
11 Defendants were arrested?

12 A. Yes.

13 Q. And did you personally participate in the search of
14 some of the or two of the residents associated with
15 Radu Miclaus?

16 A. Yes.

17 Q. I want to talk to you today about your role in
18 those searches, but first, I want to go through your
19 background.

20 What is your highest level of education?

21 A. Master's Degree.

22 Q. Where did you get a Master's Degree?

23 A. In the Romanian National Police Academy.

24 Q. Okay. So before going to the Romanian National
25 Police Academy, what did you do before that? What

Mr. Vaduva - Direct

1 education wise, what did you do before that?

2 A. Before the Academy, it is the high school.

3 Q. And what did you study in high school?

4 A. In high school: Mathematics, informatics, and
5 intensive English language.

6 Q. What is informatics?

7 A. IT let's say, IT technology.

8 Q. IT technology?

9 A. Yes.

10 Q. And you said you attended the police academy after
11 that?

12 A. Yes.

13 Q. How many years did you attend the police academy?

14 A. Four.

15 Q. And what year did you graduate from the police
16 academy?

17 A. 2010.

18 Q. And after 2010, what did you do?

19 A. I started working, it was the unit called the
20 Bucharest Brigade for Combating Organized Crime.

21 Q. Okay. And was that a unit within the Romanian
22 National Police?

23 A. Yes, that is correct.

24 Q. And within the Bucharest Brigade for Combating
25 Organized Crime, were you with a particular unit?

Mr. Vaduva - Direct

1 A. Yes. It was a smaller unit within — that was
2 combating cyber crime, in particular, car frauds and
3 skimmings.

4 Q. And what is car fraud and skimming?

5 A. Basically, we were investigating all the crimes
6 related to credit cards and fraudulent payment, stolen
7 items and credit cards, payment online, schemings, which
8 means cloning the credit card and obtaining the pin
9 number and withdraw the cash from ATMs.

10 Q. Are there different ways of using a credit card that
11 doesn't belong to someone?

12 A. Yes, that is correct.

13 Q. And how many years did you work in the Bucharest
14 Brigade that you described here?

15 A. Five years.

16 Q. And what did you do after you worked with the cyber
17 crime unit in the Bucharest Brigade?

18 A. I moved to the directory for combating organized
19 crime. That was the unit covering the whole country. It
20 was nationwide as area of competence.

21 Q. Okay. And within the directorate, were you in a
22 particular unit there?

23 A. Also, in the cyber crime unit, but to the unit that
24 was in charge of investigating the, let's say, hackings
25 and computer intrusion type of crimes.

Mr. Vaduva - Direct

1 Q. Okay. And was this another unit within the Romanian
2 National Police?

3 A. Yes, that is correct.

4 Q. When did you start at the directorate or national
5 level?

6 A. In 2015 and until December 2016 so about a
7 year-and-a-half. It was the summer of 2015.

8 Q. Okay. And what type of crimes did you investigate
9 with the cyber crime unit in the directorate office
10 within the RNP?

11 A. Type of crimes that would include computer attacks,
12 computer hackings, website attacks, botnets, all sorts
13 of crimes related to hacking, let's say, in a general
14 term.

15 Q. And how long did you say you worked for the
16 directorate?

17 A. One year-and-a-half.

18 Q. Where did you go after working for the directorate?

19 A. I applied for a position within the United States
20 Embassy in Romania for the Drug Enforcement
21 Administration.

22 Q. Was that the DEA?

23 A. The DEA.

24 Q. And is that where you presently work?

25 A. Yes, that is correct. There is an office in

Mr. Vaduva - Direct

1 Romania.

2 Q. So did you travel from Romania to travel testify —
3 to testify here today?

4 A. Yes.

5 Q. And how long have you been with the DEA with the
6 U.S. Embassy in Romania?

7 A. Since December 2016.

8 Q. Okay. And what is your title with the DEA?

9 A. Criminal investigator.

10 Q. And can you give me an example of the type of
11 cases you work on now as a criminal investigator with the
12 DEA?

13 A. The first case I worked within that office was,
14 let's say, a combination between cyber crime and drug
15 crimes?

16 And we targeted twelve websites that were
17 selling online medication, the ones that are on schedule
18 tables in Romania and also in the United States to
19 include Xanax, Valium, Diazepam, codeine and most of them
20 being opioids that drug trafficking organizations in
21 Romania was diverting from Romanian pharmacies,
22 warehouses, and distributors and then selling them online
23 via postal services, let's say, and ending up more than
24 80 percent of them in the United States but also all over
25 the world?

Mr. Vaduva - Direct

1 But the majority of the crimes were in the
2 United States. There were 75,000 packages between 2012
3 and 2017 that were sent in the United States.

4 Q. Thank you. Now, let's talk about searches of homes
5 and businesses and that kind of thing.

6 As part of your work, when you were with the
7 Romanian National Police, did you search homes and
8 apartments and businesses?

9 A. Yes.

10 Q. Roughly how many physical searches of residences or
11 businesses have you participated in?

12 A. I would say hundreds.

13 Q. Okay. Now, in Romania to do a physical search of,
14 say, a residence do you need to get a court order before
15 conducting the search?

16 A. Yes, that is correct.

17 Q. And I would like to bring up just for us — and I
18 will bring the witness a physical copy of the
19 Government's Exhibit 1410, just the first page of
20 Government's Exhibit 1410 — what is Government's Exhibit
21 1410?

22 A. This is a warrant that was approved, granted by a
23 Judge in the Court in Bucharest to conduct a search for
24 — at a certain location, assigned to a certain target,
25 let's say.

Mr. Vaduva - Direct

1 Q. Okay. And what location was this search warrant
2 for?

3 A. This was in Bucharest. In the sector 5, there is
4 six sectors in Bucharest on the street, Tiparnitei
5 number, 31st A being associated with Miclaus Radu Bogdan.

6 Q. Can you spell the name of the address?

7 A. T-i-p-a-r-n-i-t-e-i.

8 Q. Do I have it correct, that that's T as in Tom?

9 A. Yes. In English, you don't have the small comma
10 let's say underneath. It's a tsa not a ga, not a T.

11 Q. Okay.

12 A. It would be hard to explain it; don't have it.

13 Q. All right. If I could spell it and you could
14 confirm that I spelled it correctly for the court
15 reporter. Is it T-i-p-a-r-n-i-t-e-i?

16 A. Yes. That is correct.

17 Q. Okay. And then there is a number 31 A. Is that
18 correct?

19 A. Yes.

20 Q. And you said that that address is in what city?

21 A. In Bucharest.

22 Q. And Bucharest is the Capitol?

23 A. Capitol of Romania.

24 Q. Now, were you involved in obtaining that Court
25 order?

Mr. Vaduva - Direct

1 A. Yes.

2 Q. In order to obtain that Court order, did you have to
3 confirm the Romanian identification number and the birth
4 date for Radu Bogdan Miclaus?

5 A. Yes.

6 Q. And did you confirm Radu Bogdan Miclaus's birthday?

7 A. Yes.

8 Q. And what was it?

9 MR. O'SHEA: Objection.

10 THE COURT: Overruled.

11 A. It was 5th of January, 1982. We have the date of
12 births also, day, month, year, not month, day, year in
13 Romania.

14 Q. Thank you, Mr. Vaduva.

15 Now, in order to obtain the Court order, the
16 search warrant, did you first physically visit that
17 address Tiparnitei, number 31 A?

18 A. Yes.

19 Q. All right. I would like to bring up at this time
20 for the jury Government's Exhibit 1411. And what is
21 Government's Exhibit 1411?

22 A. House that we are talking about.

23 Q. Okay. Is this the house at Tiparnitei, number
24 31 A?

25 A. Yes.

Mr. Vaduva - Direct

1 Q. And it looks like there is a typo on the actual
2 exhibit. Is the address spelled correctly at the
3 top?

4 A. No.

5 Q. Okay. Is the correct address as you just provided
6 it to us?

7 A. Should be an R and then N but instead it was
8 an M.

9 Q. Okay. Now, is this a fair and accurate photograph
10 of the way the house at Tiparnitei, number 31 A, appeared
11 to be when you visited it?

12 A. Yes. This is how I remember it.

13 Q. Could we look at page 2 of this exhibit? What does
14 page 2 of this exhibit show?

15 A. It should be the 31st, which is to the left, and
16 then the number on the fence is not applied. So it
17 should be 31st A, the one to the right, and it is between
18 the number 31st and the number 33.

19 Q. But this is on the Tiparnitei street?

20 A. Yes, the apartment on the street.

21 Q. So this is the number right next to the house?

22 A. Yes.

23 Q. What does it mean when a street address has an
24 A after it?

25 A. It can have letters from A to even more when

Mr. Vaduva - Direct

1 basically the lot numbers, the houses initially were,
2 let's say — so there is even numbers and uneven numbers.
3 The even numbers are on the right side as you enter the
4 street, and the uneven numbers are on the left side as
5 you — from — from the downtown all the way to the
6 peripheral area of the city.

7 So if initially there were houses at lot
8 numbers 29, 31 and 33 but then in between a portion of
9 that land was sold to somebody else and that somebody
10 else built a house, they would be assigned with the
11 31st A because it was in between, and initially, it was
12 not counted.

13 Q. Got it.

14 A. And you can get a lot of numbers when there is going
15 to be an entrance into that lot number and it is going to
16 be multiple houses.

17 Q. Understood. Thank you.

18 Can we look at the third page of this
19 exhibit, and if you could zoom in on the photograph, the
20 whole photograph. Okay. What is this?

21 A. This is — looks like Tiparnitei Street, No. 3 as it
22 is written on the fence.

23 Q. Okay. And fourth photograph, please?

24 (Pause.)

25 Q. (Continuing) All right. When you physically

Mr. Vaduva - Direct

1 visited Tiparnitei 31 A, prior to getting the search
2 warrant, what, if anything, did you see at that address?

3 A. I saw — I remember I saw the motorcycle inside and
4 parked inside over the fence, let's say, in the
5 courtyard.

6 Q. On the other side of the fence?

7 A. A motorcycle.

8 Q. Pardon?

9 A. Motor bike.

10 Q. Okay. You said it was on the other side of the
11 fence?

12 A. Yes. Inside of the courtyard.

13 Q. How were you able to see the motorcycle if it was on
14 the other side of the fence?

15 A. Over the fence.

16 Q. And could you describe this motorcycle?

17 A. I remember it was a sports type of bike, not a
18 chopper but not a super sport, and I remember it being
19 dark colored. I don't remember the make, but I remember
20 I searched the license plates to confirm the owner.

21 Q. All right. And who was the motorcycle registered
22 to?

23 A. To Radu Miclaus.

24 Q. That's Radu Bogdan Miclaus?

25 A. Yes.

Mr. Vaduva - Direct

1 Q. On September 18, 2016, were you part of the team
2 that conducted a search on Tiparnitei 31 A?

3 A. Yes.

4 Q. And was anyone from the residence present during
5 that search?

6 A. Yes. It was only the father of Radu Bogdan Miclaus.

7 Q. Miclaus' father?

8 A. Yes.

9 Q. And was there anyone else present at the residence
10 when you got there?

11 A. No, just the father.

12 Q. Did you seize any items from Tiparnitei, number
13 31 A?

14 A. Yes. I remember I did.

15 Q. And what did you do with the items that you seized
16 from Tiparnitei 31 A?

17 A. The procedure all the time is you basically put them
18 in plastic bags, depending on the size of the items and
19 seal them, and after that, we took them to the
20 prosecutor's office that was in charge of the
21 operation.

22 Q. Okay. So you brought them to the prosecutor's
23 office?

24 A. Yes, that is correct.

25 Q. All right. Now, I would like to show you what has

Mr. Vaduva - Direct

1 been marked as Government's Exhibit 1413, and I think we
2 can show this to the jury as well.

3 And what is Government's Exhibit 1413?

4 A. This is one of the entrances to the apartment
5 building where Radu Bogdan Miclaus was also living.

6 Q. And was this the next location you went to on
7 September 28, 2016?

8 A. Yes, that is correct.

9 Q. Okay. And was the address here U-v-e-r-t-u-r-i-i?

10 A. Yes.

11 Q. How is that pronounced?

12 A. Uverturii.

13 Q. Uverturii?

14 A. Uverturii.

15 Q. And what was the full address?

16 A. The full address was the Boulevard Uverturii No. 4,
17 apartment building C3, entrance No. 4, floor 4, which
18 would be your fifth floor because we don't count the
19 ground floor, apartment 70, sector 6.

20 Q. Okay. And is that also in Bucharest, Romania?

21 A. Yes.

22 Q. Can we look at the second page?

23 And what do we see here on the second page
24 of Government's Exhibit —

25 A. This is a larger picture of the apartment building.

Mr. Vaduva - Direct

1 Q. And can we look at the third page?

2 A. This is still basically this entrance No. 4, was at
3 the end of the apartment building, but then, to the left,
4 there were three other entrances. So it goes more to the
5 left of this apartment building.

6 Q. And what does this photograph depict?

7 A. I'm sorry. I didn't —

8 Q. What does this photograph depict? What do we see in
9 this photograph?

10 A. The floor No. 4, so the fifth floor, as you would
11 number it, the apartment was located.

12 Q. Okay. Is there another one on this one?

13 A. So it was the last floor.

14 Q. Okay. And what does this last photograph
15 show?

16 A. To the right, it shows the No. 4 assigned to the
17 street number, and to the left, there is a plaque with
18 the apartment building number, which is C3 and, again,
19 the street number and the Boulevard Uverturii 3, No. 4,
20 and in Romania, in general, you would see it doesn't —
21 you can't quite distinguish — but there is the No. 4
22 entrance, and they put in the apartment number.

23 So it would be, let's say, from apartment
24 No. 40 to apartment No. 60. So you would know what
25 numbering of the apartments would be inside.

Mr. Vaduva - Direct

1 Q. Okay. And do all the photographs we have looked at
2 fairly and accurately depict the locations that you
3 searched in this case in 2016?

4 A. Yes.

5 Q. Okay. When you arrived at the Uverturii building
6 entrance, was the search already in progress?

7 A. No.

8 Q. What was happening at the Uverturii building No. 4
9 entrance here when you arrived?

10 A. Two other colleagues, two other police officers,
11 were waiting for Radu Miclaus Bogdan to be brought at the
12 location because he was stopped in traffic as I remember
13 in a county somewhere in the middle of Romania.

14 He was coming from the West, let's say, of
15 Romania, and normally, this would be the procedure. If
16 you don't have the suspect or somebody from the family
17 inside the house and we know that, we won't break and use
18 force to put the door down and do it without their
19 presence.

20 So basically, we waited for him, those two
21 colleagues waited for him, and I joined them because at
22 that time both of them were not from any — from the
23 cyber unit, and they sent me to basically help and have
24 the knowledge to be present there as the cyber police
25 officer.

Mr. Vaduva - Direct

1 Q. So that's standard procedure in Romania, to wait for
2 the person whose house you are searching or their family
3 before you do a search?

4 A. It is standard, but it depends on the type of
5 crime that is committed, and any of the goods or
6 things that are inside may disappear, or somebody else
7 would come or something would danger collecting the
8 evidence, but in this case, it wasn't so. So we were
9 okay to wait.

10 Q. And roughly how long did you wait from for Miclaus
11 to arrive from the time you got there?

12 A. I remember it was afternoon, I think, after 3:00
13 p.m.

14 Q. Do you recall roughly, was it hours, half hour?

15 A. Normally, in Romania, we enter at 6:00 a.m. for all
16 of the search warrants. The Romanian penal codes state
17 you can enter for a search warrant between 6:00 a.m. and
18 8 p.m., and we go as early as possible?

19 So basically, if we have all of them in
20 house, not awake, so all of the search warrants in the
21 case started at 6:00. So we waited quite a lot until
22 3:00 p.m. as you can imagine for him to come in from
23 Bucharest and participate in the search warrant.

24 Q. Okay. So you said you didn't start until around
25 3:00 p.m.?

Mr. Vaduva - Direct

1 A. Yes.

2 Q. But did Miclaus eventually arrive?

3 A. Yes.

4 Q. And when Miclaus arrived, was he given an
5 opportunity to contact a lawyer or a trusted
6 person?

7 A. Yes. That's also standard procedure according to
8 the Romanian penal code.

9 Q. What is a trusted person?

10 A. That's exactly how it is named, and basically, he
11 can call a friend; he can call a neighbor. He can call
12 somebody he knows and would feel comfortable with
13 participating in case, let's say, he was never involved
14 in such a matters or if he is anxious, let's say, and
15 wants somebody to be present with him during the search
16 warrant.

17 Q. So did you then after 3:00 p.m. wait for a lawyer or
18 trusted person to arrive?

19 A. The penal code also says in case of a trusted
20 person, it doesn't say the amount of time you need to
21 wait before the person comes, but in the case of a
22 lawyer, you need to wait two hours.

23 So if the suspect wants to have a lawyer
24 present at the location, he will make the call or the
25 police officer would make the call. You would note down

Mr. Vaduva - Direct

1 exactly the hour the call was made and wait two hours.

2 If those two hours come, you can start.

3 Q. In this instance, did you wait for a lawyer or
4 trusted person to arrive?

5 A. No. It was not the case because Radu Miclaus Bogdan
6 waived this right and said he is comfortable to be just
7 himself during the search warrant.

8 Q. Okay. And how did you get in to the Uverturii
9 apartment?

10 A. With his help, with the keys that he had.

11 Q. So Radu Miclaus had the keys to the apartment?

12 A. Yes.

13 Q. And he opened the door?

14 A. Yes.

15 Q. Who was present in the Uverturii apartment when the
16 search began?

17 A. Myself, the two other colleagues, and Radu Miclaus
18 Bogdan.

19 Q. Okay. And anybody else besides yourself, Miclaus,
20 and the two other colleagues?

21 A. No.

22 Q. What rooms were in the Uverturii apartment?

23 A. It was an apartment composed of three rooms. That's
24 how we count them, namely a living room and two bedrooms,
25 and of course, the hallway, bathroom, and kitchen.

Mr. Vaduva - Direct

1 Q. And was Miclaus present in each room when that room
2 was searched?

3 A. Yes. That's also standard procedure.

4 Q. Did you seize any digital devices like hard drives,
5 phones, routers from the Uverturii apartment?

6 A. Yes.

7 Q. Okay. And last night did you meet with him with me
8 and did you have an opportunity to review the digital
9 devices that are on the table in front of you to confirm
10 that they were the devices you seized from the Uverturii
11 apartment?

12 A. Yes.

13 Q. And are these the devices that you seized from the
14 Uverturii apartment?

15 A. Yes.

16 Q. How were you able to tell that these were
17 the devices that you seized from the Uverturii
18 apartment?

19 A. By remembering the looks of them, first of all, and
20 also by checking the serial numbers on the report or
21 inventory sheet that was written with that occasion, with
22 the actual serial numbers on the devices.

23 Q. So last night you compared serial numbers in your
24 report to the serial numbers on the actual devices?

25 A. Yes.

Mr. Vaduva - Direct

1 Q. And did they match?

2 A. Yes, all of them.

3 Q. Okay. Now, I want to go through some of these or
4 all of these with you. And I would like to hand you what
5 has been previously marked as Government's Exhibit 2424,
6 Government's Exhibit 2341, and Government's Exhibit 2317.

7 What are these three exhibits in front of
8 you?

9 A. The three hard drives that were extracted from the
10 PC desktop computer.

11 Q. Okay. Now, I am going to ask you about everything
12 you just said, but how large is each one of these hard
13 drives?

14 A. Each of them has two terabyte for 2000 gigabytes, so
15 six terabytes or 6,000 gigabytes in total.

16 Q. This is a total of six terabytes of hard drive
17 space?

18 A. Yes.

19 Q. And do you know how large a terabyte is?

20 A. Yes. It is quite large.

21 Q. Quite large. Can you be more specific? In paper,
22 how many pages of paper would a terabyte be?

23 A. Hundreds of thousands, but if we are talking movies,
24 it would be even more space than documents. Documents
25 you could put quite a lot.

Mr. Vaduva - Direct

1 Q. With documents like a Word document —

2 A. Yes. PDFs or —

3 Q. How many documents could you get on a terabyte hard
4 drive?

5 A. I don't know, maybe couple hundred thousand.

6 Q. Did you find these hard drives out like they are now
7 or in a computer?

8 A. No. They were in the computer.

9 Q. All right. And can you describe the computer that
10 they were in?

11 A. I remember that the central unit as we call it was a
12 black one, and it was sitting next to a desk, and it was
13 in the bedroom.

14 Q. Okay. You called it a central unit. Was this a
15 laptop computer or a desktop?

16 A. No, desktop, in the tower of the desktop.

17 Q. These were in the tower of the desktop
18 computer?

19 A. Yes.

20 Q. And you said the computer, where was the computer
21 located?

22 A. In one of the two bedrooms.

23 Q. And was there a monitor attached to this
24 tower?

25 A. Yes.

Mr. Vaduva - Direct

1 Q. And was there a keyboard attached?

2 A. Yes.

3 Q. And was there a mouse attached?

4 A. Yes.

5 Q. And was the computer plugged in?

6 A. No.

7 Q. It was not plugged in at the time?

8 A. No.

9 Q. Did you seize the entire computer or just the hard
10 drive?

11 A. Just the hard drives.

12 Q. Why did you seize just the hard drives?

13 A. First of all, because the computer was shut down, we
14 didn't — there is also a procedure that basically if a
15 computer is not shut down, we would call the colleagues
16 from the forensics unit and try to get the live RAM
17 acquisition, which would be the other memory of the
18 computer and try to get all the data from that RAM, but
19 that only is available if the computer is open.

20 If it is shut down, that erases every time
21 you read through the computer, so it wasn't essential.
22 The only storageable data that would have been usable to
23 the case as evidence would have been the hard drives
24 themselves.

25 And secondly, space wise, because it was

Mr. Vaduva - Direct

1 quite a large desktop computer, and as I previously said,
2 we needed to seal all of them in plastic bags, and we
3 also thought at that moment that being not a Romanian
4 case, being a case from the United States, it would have
5 had to be shipped as a response to the M-IAT request.

6 Q. Okay. So there was a tower.

7 All the data was — was all the data
8 available in that tower in these three hard drives?

9 A. All the useable data.

10 Q. What do you mean "all the usable." Was there any
11 data not usable in the tower?

12 A. Yes. Some don't contain data at all.

13 Q. So there was no other information in the tower
14 itself that you didn't seize?

15 A. No.

16 Q. Okay. I want to show you what has previously been
17 marked as Government's Exhibit 255. What is Government's
18 Exhibit 255?

19 A. A Samsung mobile phone, a galaxy S3 model.

20 Q. And where did you find Government's Exhibit 255?

21 A. In the same room, in the same bedroom. I think it
22 was in one of the drawers in the desk.

23 Q. Okay. And now, I would like to show you what
24 has previously been marked as Government's Exhibit
25 1415.

Mr. Vaduva - Direct

1 MR. LEVINE: Let the record reflect we are
2 making our best efforts to protect the stand from
3 scratching.

4 THE COURT: Very happy to hear that.

5 BY MR. LEVINE:

6 Q. I am showing you what has previously been marked as
7 Government's Exhibit 1415. What is Government's Exhibit
8 1415?

9 A. This would be a wireless router that is supposed to
10 have three original antennas. Right now the middle has
11 only the original, and to the right, there is an extra
12 one, and to the left of the cable, there is another
13 antenna that is basically amplifying the strength of the
14 router.

15 Q. Can you explain to the jury where did you find this
16 exhibit?

17 A. This was also in the same bedroom but it was pretty
18 strange because it was hanging at the window curtain with
19 the clothes hanging pins on the curtain so up next to the
20 window.

21 Q. It was pressed up against the window?

22 A. No. Basically, it was the window, the curtain, and
23 it was tied to the curtain.

24 Q. Tied to the inside of the curtain?

25 A. Outside. You would see it, but the curtain was

Mr. Vaduva - Direct

1 similar to what we have here, transparent ones.

2 Q. So you would see it from the inside of the
3 apartment?

4 A. Yes.

5 Q. It was on the inside of the apartment, and then was
6 the curtain, and then was the glass?

7 A. Yes.

8 Q. Okay. And you said what was it that was holding it
9 in place against the curtain?

10 A. Pins that you use to hang the clothes to dry.

11 Q. So clothes pins?

12 A. Clothes pins, yeah.

13 Q. And roughly how many searches did you say you
14 conducted in Romania?

15 MR. GOLDBERG: Objection.

16 THE COURT: Overruled. You may answer.

17 A. Hundreds.

18 Q. And did you ever see an antenna like this during any
19 of the other searches you conducted?

20 MR. GOLDBERG: Objection.

21 THE COURT: Overruled.

22 THE WITNESS: No.

23 BY MR. LEVINE:

24 Q. I am going to take this.

25 A. Okay.

Mr. Vaduva - Direct

1 MR. LEVINE: Now, I will show the witness
2 previously marked Government's Exhibit 2047, 2048, 2049,
3 2050, 2051, and 2052.

4 BY MR. LEVINE:

5 Q. What are these, Mr. Vaduva?

6 A. These are also wireless routers but standard ones,
7 six of them.

8 Q. Okay. Where did you find these six routers?

9 A. I remember there were five in the living room and
10 another one — I don't know exactly which of them — was
11 also in the bedroom. It was on top of the dresser.

12 Q. Okay. In the hundreds of searches you conducted in
13 Romania, had you ever seen an apartment with six or seven
14 routers prior to this?

15 A. No. Usually, it is one or no more than two. If it
16 is a house, you may find two. If it is an apartment
17 building, usually you find one because it covers enough
18 area to cover a signal.

19 Q. And was this an apartment or a house?

20 A. An apartment.

21 Q. Okay. Thank you. Okay.

22 MR. LEVINE: I want to show this witness
23 what has previously been marked as Government's Exhibit
24 1414, and let's bring it up on the screen for the witness
25 right now.

Mr. Vaduva - Direct

1 THE COURT: Just for the witness, did you
2 say?

3 MR. LEVINE: Do you have an objection?
4 Let's bring it up to the witness first, your Honor.

5 MR. O'SHEA: Objection. May we approach?

6 THE COURT: You may.

7 (Side bar held on the record.)

8 MR. O'SHEA: All right. Here is my
9 objection. This translation of this report, which starts
10 on page 8, Judge, indicates that it has got information
11 about this being the residence of Radu Bogdan Miclaus.
12 That's hearsay pure and simple.

13 On page 9, it says the search property is
14 made up of three rooms, corners, annexes used by Radu
15 Bogdan Miclaus, Bogdan Nicolescu about who you declares
16 that he only came to the apartment once in a while.
17 Again, hearsay.

18 Then, I think on the inventory sheet here it
19 says, for instance, the phone is issued by Radu Bogdan
20 Miclaus. So that's all hearsay without an exception
21 that I am aware of because I don't know who the declarant
22 is.

23 MR. LEVINE: I will ask, so the declarant is
24 Miclaus, who is a party opponent, and I can ask the
25 witness who was there who provided that information.

Mr. Vaduva - Direct

1 THE COURT: Because as of right now, the
2 objection is well taken, so —

3 MR. O'SHEA: As long as the information came
4 from Radu Miclaus and only Radu Miclaus and not any other
5 agent or investigator, we have to be — I believe we
6 should be very careful about the foundation.

7 THE COURT: And I am sustaining your
8 objection at this point, which is why I am not going to
9 allow the jurors to see it yet.

10 MR. LEVINE: Okay. That's fine, your
11 Honor.

12 (Side bar concluded.)

13 BY MR. LEVINE:

14 Q. I am going to hand you a physical copy of the
15 Government's Exhibit 1414, so you have the whole thing.

16 THE COURT: Folks, it is not on your screen,
17 correct?

18 (Jurors answered no).

19 THE COURT: Okay.

20 BY MR. LEVINE:

21 Q. And can I ask you, what is Government's Exhibit
22 1414?

23 A. This is the standard report that we are drafting
24 while conducting a search warrant.

25 Q. Okay. And were you personally involved in preparing

Mr. Vaduva - Direct

1 this report?

2 A. Yes.

3 Q. What was your role in preparing this report?

4 A. The handwriting, it is not mine. I was the one that
5 actually wrote the one on Tiparnitei, but on this one was
6 the other colleague, Vilculescu Bogdan, the last of the
7 three that wrote it, and I was the one that was basically
8 was inventorying the goods and also checking the serial
9 numbers and spelling them out to him, while he was there
10 writing it.

11 Q. So you would read aloud the serial numbers of each
12 of these devices?

13 MR. O'SHEA: Objection to the form of the
14 question.

15 THE COURT: I am going to allow that so I
16 can understand. Is that what you said, sir?

17 THE DEFENDANT: Yes.

18 THE COURT: Okay. Thank you.

19 BY MR. LEVINE:

20 Q. And your colleague would write them down on the form
21 as you read them aloud?

22 MR. O'SHEA: Objection.

23 THE COURT: Overruled. I understand.

24 Mr. O'Shea, for this one I am going to allow it.

25 THE WITNESS: Just as a further explanation,

Mr. Vaduva - Direct

1 normally this is what we do all the time because it would
2 be hard for only one police officer to look at the
3 physical evidence and also write it down, but then, at
4 the end, everybody reads it, and everybody double checks
5 it, the ones that sign it.

6 BY MR. LEVINE:

7 Q. Did you read it, and did you double check it while
8 you were still at the Uverturii apartment?

9 A. Yes, that is correct.

10 Q. Okay. And who signed Government's Exhibit 1414?

11 A. The three of us as police officers and Bogdan Radu
12 Miclaus after he also read it.

13 Q. All right. And can you tell me who the three police
14 officers were who signed?

15 A. It would be police subcommissioner Borld Ionun.

16 Q. And could you spell that for the court reporter.

17 A. B-o-r-l-d.

18 Q. It is B-o-a-l —

19 A. No, no. Sorry. B-o-r-l-d, I-o-n-u-n.

20 Q. Okay. And so that was one officer. What was the
21 next officer?

22 A. The next one was me, Police Inspector Vaduva Bogdan,
23 and the last one that actually wrote it is police
24 subinspector. This is the sublieutenant of the ranking,
25 Vilculescu Bogdan, which would be V-i-l-c-u-l-e-s-c-u,

Mr. Vaduva - Direct

1 B-o-g-d-a-n.

2 Q. Okay. And did these people — strike that.

3 Including — and was one of the four people
4 who signed it Bogdan Miclaus?

5 A. Yes.

6 Q. Or Radu Bogdan Miclaus?

7 A. Yes.

8 Q. And did these four people sign every page of
9 Government's Exhibit 1414?

10 A. Yes. This is how we do it all the time, so
11 basically, we acknowledge with the person involved
12 everything that was written on every page.

13 Q. Okay. And was Miclaus in handcuffs at the time he
14 signed this form?

15 A. No. He was never in handcuffs.

16 Q. Did you see or hear anyone threaten Miclaus?

17 A. No.

18 Q. Did you see or hear anyone yelling at Miclaus?

19 A. No.

20 Q. Did you see or hear anyone offer Miclaus something
21 of value to sign this form?

22 A. No.

23 Q. All right. If you turn to page 3 of the form, there
24 is some information there about the ownership of the
25 apartment.

Mr. Vaduva - Direct

1 Who provided that information?

2 A. I don't see information about ownership of the
3 apartment. There is information about ownership of the
4 computer and of the routers.

5 Q. Okay. Who provided that information about ownership
6 of the computer and the routers?

7 A. Bogdan Radu Miclaus himself confirmed that he was
8 the one using them.

9 Q. And if we could turn to the English translation.
10 There is some information provided about a Linksys router
11 serial number CL7BIG C30244, do you see that?

12 A. Yes.

13 Q. Who provided that information?

14 A. But he is mentioning about all of the above, the
15 five routers, not only the Linksys one.

16 Q. Okay.

17 A. So —

18 Q. Okay. But who provided the information?

19 A. Himself. He stated that in the —

20 Q. Wait. I am just asking you who provided the
21 information; not what is the information.

22 A. Radu Bogdan Miclaus.

23 Q. Okay. And towards the top, did somebody indicate
24 that the computer, whose property the computer was, and
25 that he was the only one who uses it?

Mr. Vaduva - Direct

1 A. Radu Miclaus Bogdan confirmed that. Sorry, this is
2 also somehow standard procedure we tend to ask, so we
3 have it in writing who is the one using in case there is
4 multiple people in the house.

5 But in this case, it was only him, and
6 he confirmed those are goods were used by him and him
7 alone.

8 Q. Okay.

9 MR. LEVINE: Your Honor, at this point, can
10 I show the exhibit to the jury?

11 THE COURT: Mr. Goldberg?

12 MR. GOLDBERG: No objection.

13 THE COURT: Mr. O'Shea?

14 MR. O'SHEA: One moment, please.

15 (Pause.)

16 MR. O'SHEA: Objection.

17 THE COURT: For the same reasons you
18 articulated at the side bar?

19 MR. O'SHEA: Yes, ma'am.

20 THE COURT: Objection overruled.

21 I will allow it to be published, admitted
22 and published.

23 MR. LEVINE: Can we show this to the jury,
24 your Honor?

25

Mr. Vaduva - Direct

1 MR. LEVINE: Thank you so much. Now what we
2 are looking at is page 4 of the translation?

3 THE COURT: I apologize. What number are we
4 on?

5 MR. LEVINE: We are on Government's Exhibit
6 1414 and looking at page 8 of the exhibit, which is in
7 the English translation.

8 THE COURT: Thank you.

9 MR. O'SHEA: And your Honor, without — not
10 to interrupt, the exhibit itself is, I believe, 14 pages
11 long. We are just talking about one page here as far as
12 publishing and admission. I know that's two separate
13 things. I don't know that the whole document comes in
14 yet because it refers to many other matters.

15 THE COURT: Fair enough.

16 The pages that have already been testified
17 to will be admitted, and I will allow them to be
18 published.

19 BY MR. LEVINE:

20 Q. While we are on this page, what did Radu Bogdan
21 Miclaus say with respect to his computer?

22 A. He declared it is a computer owned by him and
23 private property, and he is the only one using it.

24 Q. Okay. If we could go to the first page of the
25 translation.

Mr. Vaduva - Direct

1 And does this first page of the translation
2 accurately state the address that you were searching at
3 Uverturii Boulevard?

4 MR. O'SHEA: Objection, your Honor.

5 THE COURT: Sustained.

6 MR. O'SHEA: Could we not show this to the
7 jury?

8 THE COURT: That's not why I sustained your
9 objection.

10 MR. O'SHEA: Understood, Judge.

11 THE COURT: Bring the entire exhibit up to
12 me and resolve the entire —

13 MR. O'SHEA: Can it be taken down?

14 THE COURT: Yes.

15 (Side bar held on the record.)

16 THE COURT: This Court is satisfied that the
17 portions Mr. O'Shea discussed at the prior side bar are,
18 in fact, admissible. They are non hearsay.

19 So do you have any other objection to the
20 exhibit, Mr. O'Shea?

21 MR. O'SHEA: Yes. He was just showing a
22 page — what page was that? So on page 6 of 9, for the
23 record, it basically says — talks about an investigation
24 suspect Defendant person named Radu Miclaus. That's
25 definitely information from somebody other than Radu

Mr. Vaduva - Direct

1 Miclaus. No question in my mind.

2 THE COURT: May I see it?

3 MR. LEVINE: Yes.

4 (Pause.)

5 THE COURT: Okay. So your objection to page
6 6 of 9 of Exhibit 1414 is that it contains hearsay, and
7 the hearsay specifically is that the residence in
8 question is of Radu Bogdan Miclaus.

9 MR. O'SHEA: Here, we have a problem. The
10 exhibit that I am looking at, Exhibit 1414, is not 9
11 pages long but, in fact, 12 pages long.

12 MR. LEVINE: As of last night, I removed the
13 order from the exhibit.

14 MR. O'SHEA: Okay. It is repaginated.
15 Okay. Okay.

16 Just so we get clear, the exhibit that I am
17 holding, which was one of the original Exhibits 1414 as
18 marked, has on it on the first page that we are talking
19 about here — that would be on this one — let me just
20 point to the one in your hand.

21 On page 6 of 9 that we were talking about,
22 it says "suspect" — this report was obviously generated
23 based on information that generated the search warrant
24 and not necessarily information that came from Radu
25 Miclaus himself.

Mr. Vaduva - Direct

1 MR. LEVINE: With respect to this particular
2 page, your Honor, it just says suspect, defendant, or
3 person, so there is nothing —

4 THE COURT: Let's start from the beginning.
5 This is — is this akin to a United States of America
6 police report?

7 MR. LEVINE: I don't think so, your Honor.
8 I think this is an inventory form.

9 THE COURT: I'm sorry, folks.

10 MR. LEVINE: I don't think so. This is
11 akin to an inventory form done at a jail or any other
12 location.

13 THE COURT: Well, this page certainly
14 doesn't indicate that, and the fact that you said you
15 don't think so, it looks to me like it is a police
16 report, and police reports aren't coming in. This does
17 not look like an inventory sheet that's attached to a
18 search warrant.

19 MR. LEVINE: So your Honor, there is no
20 search warrant here. The search warrant is a separate —
21 was Exhibit 1410.

22 We didn't admit it, and if I could go
23 through this briefly, it lists the item seized with a
24 serial number and indicates that the subject Miclaus,
25 there is a place for him to write an objection and shows

Mr. Vaduva - Direct

1 he did not write any objection.

2 A police report would be a report of an
3 incident what the police officer saw. I think this is
4 very different —

5 THE COURT: You are testifying now. I
6 haven't heard that from this witness.

7 MR. LEVINE: Okay. I suggest we just made
8 3, 4, 7, and 8 which is his admission and signature.

9 THE COURT: And again, I need to hear
10 that from the witness before I can say that this is
11 admitted.

12 MR. LEVINE: Okay. So let me —

13 THE COURT: But the portion that Mr. O'Shea
14 has pointed out, unless you can explain it to me, it
15 certainly appears as if it is akin to a police report,
16 the officer's statements that go into a police report
17 about his or her investigation, and that's what my
18 problem is.

19 MR. LEVINE: So I will stick to page 3, 4,
20 7, and 8 and ask the witness.

21 THE COURT: Go off the record for George.

22 (Discussion held off the record.)

23 (Side bar concluded.)

24 THE COURT: Without objection we are looking
25 at pages 7, 8.

Mr. Vaduva - Direct

1 MR. LEVINE: 3 and 4.

2 THE COURT: 3, 4, 7, and 8.

3 Mr. O'Shea, correct?

4 MR. O'SHEA: Correct, your Honor.

5 THE COURT: All right.

6 BY MR. LEVINE:

7 Q. Okay. So Mr. Vaduva, page 7 here is the English
8 translation of page 3 of your form.

9 Let me just clarify, can you read the
10 English translation?

11 A. The whole page?

12 Q. No. Do you have the ability — I'm sorry.

13 You speak English very, very well, but I
14 just want to confirm, do you have the ability to read the
15 English translation?

16 A. Sure.

17 Q. Okay. I am not asking you to read the whole
18 page.

19 Did Radu Miclaus say anything about whose
20 residence this was on this translated into English on
21 page 7 of this exhibit?

22 A. At that time, he mentioned that he is coming from
23 time to time every once in a while because he was living
24 at that time with a girlfriend —

25 Q. Okay. So —

Mr. Vaduva - Direct

1 A. — in the girlfriend's apartment.

2 Q. So who was saying this to you?

3 A. Radu Bogdan Miclaus.

4 Q. And you used the word "he," and I want to be
5 specific.

6 A. I'm sorry.

7 Q. Who did he say came to the apartment from time to
8 time?

9 A. Radu Bogdan Miclaus.

10 Q. Did he say that anyone else came to the apartment
11 from time to time?

12 A. No, not that I am aware of.

13 Q. What did he say, if anything, about Bogdan Nicolescu
14 looking at the —

15 MR. GOLDBERG: Objection.

16 THE COURT: Sustained.

17 BY MR. LEVINE:

18 Q. Did he indicate anything about anyone else coming to
19 the apartment?

20 MR. GOLDBERG: Objection.

21 THE COURT: Overruled.

22 THE WITNESS: No, not that I remember.

23 BY MR. LEVINE:

24 Q. If we could go to page 3 of the original Romanian —
25 looking at page 3, did Radu Bogdan Miclaus say anything

Mr. Vaduva - Direct

1 about who rented the apartment?

2 MR. O'SHEA: Objection. Side bar.

3 THE COURT: On this?

4 MR. O'SHEA: I think so, Judge.

5 THE COURT: All right.

6 (Side bar held on the record.)

7 MR. O'SHEA: If he is using this document to
8 refresh this witness' recollection, which appears he is
9 doing, the foundation has not been set.

10 Would it assist you, a document to refresh
11 your recollection? Answer: Yes. He can't just ask
12 right in there.

13 MR. LEVINE: I will ask a different question
14 on the record.

15 (Side bar concluded.)

16 BY MR. LEVINE:

17 Q. To whom did Miclaus tell what we see on page 3 in
18 Romanian and page 7 in English?

19 A. Basically, we were all three officers standing with
20 him in the same room because, as I mentioned, nobody was
21 present anywhere else except where he was also present?

22 And I can confirm it was I asking the
23 questions and sometimes also Borld Ionun because he was
24 also the higher ranking officer, and he was also involved
25 in the procedures, so both of us would ask.

Mr. Vaduva - Direct

1 Q. And were you there to hear the answers?

2 A. Of course. As I said, all four were present all the
3 time in the same room.

4 Q. Okay. And do you recall Miclaus saying anything
5 about Bogdan Nicolescu?

6 MR. O'SHEA: Objection.

7 THE COURT: Sustained.

8 BY MR. LEVINE:

9 Q. Did you recall Miclaus saying anything else about
10 who owned or rented the apartment?

11 MR. O'SHEA: Objection.

12 MR. GOLDBERG: Objection.

13 THE COURT: Sustained.

14 BY MR. LEVINE:

15 Q. What else, if anything, did Miclaus say?

16 A. Right now, if I remember, only about the seized
17 goods from the apartment that he mentioned, and we asked
18 the questions, also.

19 And normally, everything that we asked and
20 connected with the case, it is going to be written down
21 in the report and note everything that he states will
22 also be written down in the report.

23 Q. Okay. If we could go to page 7 of this exhibit?

24 MR. O'SHEA: Objection, your Honor.

25 THE COURT: Sustained. Sustained. Please

Mr. Vaduva - Direct

1 don't show it.

2 MR. LEVINE: Can we have a quick side bar?

3 Sorry.

4 (Side bar off on the record.)

5 BY MR. LEVINE:

6 Q. All right. Let me hand you what has been marked
7 Government's Exhibit 1414. If you could turn to the last
8 page of the original Romanian, what is the blank space on
9 page 9 of Government's Exhibit 1414 or on the last page
10 of the Romanian?

11 MR. O'SHEA: What page, Brian, again?

12 MR. LEVINE: The last page of the form or
13 the last page of the translation.

14 THE WITNESS: Are we talking about the
15 Z marking on the blank?

16 BY MR. LEVINE:

17 Q. The blank space there, what he is that blank space
18 for?

19 A. This phrase over here states that the person that
20 had participated and — and I am reminding everybody just
21 a standard form that we print and fill in, so the person
22 or persons in this case being Miclaus Radu Bogdan has
23 taken part in the search warrant?

24 And they don't have any objections or
25 perform any explanations in regards with the way the

Mr. Vaduva - Direct

1 search warrant was conducted nor does he have any
2 objections or issues regarding the details that were
3 written down in the present report, and if they would
4 have something, they declare that.

5 And if he put that, the Z marking means that
6 he has nothing to say against what happened nor that he
7 has any arguments.

8 Q. Okay. Did Miclaus write —

9 THE COURT: May I interrupt? May I see
10 that, sir?

11 (Pause.)

12 MR. LEVINE: Okay. Your Honor, would it
13 help if I withdrew the question?

14 THE COURT: No. No, no, no.

15 BY MR. LEVINE:

16 Q. Okay. Did Miclaus write down any objection to the
17 search?

18 A. No.

19 Q. Did Miclaus write down anything about the search on
20 the form?

21 A. No.

22 Q. Was Miclaus given an opportunity to write down
23 anything on the form?

24 A. Of course.

25 Q. Now, were all the routers you testified to in

Mr. Vaduva - Direct

1 substantially the same condition as when you seized them
2 in Romania in 2016?

3 A. Yes.

4 MR. LEVINE: And I want to hand the witness
5 what has previously been marked as Government's Exhibit
6 2054.

7 BY MR. LEVINE:

8 Q. What is Government's Exhibit 2054?

9 A. This is the type of sealing matter that we use. We
10 use clay and either like a — something to basically melt
11 it, and we are going to put it on this piece of
12 cardboard?

13 And so the whole process is putting these
14 goods in a bag, tying it up with rope, putting the rope
15 in between the cardboard, tying it. Then also here,
16 putting the seal?

17 And basically, if you would like to open the
18 bag, you couldn't do it without breaking the seal. So
19 that's our way to, one of — not the only way — to seal
20 and have the goods and the digital evidence kept in
21 exactly the same condition and shape as it was at the
22 moment of the search warrant.

23 Q. Okay. And once — and did you bag up and seal these
24 physical exhibits we looked at here on the table and used
25 the seal on them?

Mr. Vaduva - Cross

1 A. Yes, that is correct.

2 Q. And once you bagged up and sealed these items, where
3 did you bring them?

4 A. To the prosecutor's office that was handling the
5 matter.

6 MR. LEVINE: No further questions for this
7 witness.

8 THE COURT: Mr. Goldberg?

9 MR. GOLDBERG: Thank you.

10 CROSS EXAMINATION

11 BY MR. GOLDBERG:

12 Q. You mentioned earlier in your testimony that you
13 were responding to an M-IAT request?

14 A. Yes, that is correct.

15 Q. An M-IAT request is a request that the United States
16 or another country in Romania had a treaty to make to
17 gather evidence?

18 A. Yes. That is correct, it is a legal agreement.

19 Q. On behalf of the requesting country, correct?

20 A. Yes, and that is correct.

21 Q. And the requesting country can ask the target
22 country to search a place or a person?

23 A. Yes, that is correct.

24 Q. Intercept phone lines?

25 A. Yes. That is correct, and then I was mentioning,

Mr. Vaduva - Cross

1 this happens only if the crime that is mentioned in the
2 M-IAT has the equivalent in the country that it is
3 requested from.

4 So if the crime doesn't exist in Romania, we
5 cannot obtain judge warrants and the other authorizations
6 to conduct the wiretap, for example.

7 Q. Fair enough.

8 And the type of fraud the United States was
9 investigating was is a crime in Romania?

10 A. Yes.

11 Q. So you had no problem filling the M-IAT request,
12 correct?

13 A. Yes.

14 Q. So the government that is requesting can ask you to
15 search a person or place, and you already answered that,
16 intercept telephone communications?

17 A. Yes.

18 Q. Intercept internet communications?

19 A. Yes.

20 Q. Enter and place a listening or video device within a
21 home?

22 A. Yes. That is also correct, but it depends on the
23 type of crime. So it needs to be from the organized type
24 of crimes, crime or serious type of criminal activity.

25 If we are talking about regular theft, it

Mr. Vaduva - Cross

1 would not be authorized by the judge. They specify the
2 exact crimes that are eligible to obtain such type of
3 measures, which are considered also very intrusive in the
4 personal life.

5 Q. But a judge in Romania has to approve those requests
6 as well?

7 A. All of them.

8 Q. Now, the reports you were just going over, 1414 and
9 1410 with Mr. Levine, those were generated at the time of
10 the search or — they were generated at the time of the
11 search, correct?

12 A. Yes, that is correct.

13 Q. And was there another report generated at the same
14 time, a narrative telling a story of what happened and
15 how the police entered the residence and what happened
16 once they got in there, or are these exhibits the record
17 of the search?

18 A. Yes. This is the only record of the search. The
19 only extra report that you would see is the inventory of
20 all of the assets that were seized during the whole
21 search operation from all of the targets.

22 But that would be just the inventory of the
23 goods to be passed to the United States authorized, so
24 that's it in regards to the search warrants.

25 Q. So now, we are about two and-a-half years later,

Mr. Vaduva - Cross

1 right, roughly?

2 A. Yes.

3 Q. Okay. So you remember some of the details of these
4 searches but not every detail. You have to refresh your
5 memory by looking at the reports?

6 A. That is correct.

7 Q. So that is basically a report of the police
8 activity?

9 A. That is correct.

10 Q. And the only one that exists?

11 A. Yes.

12 Q. Okay. With regard to the routers — and I am not
13 going to go through every number, there is a table here,
14 the number of devices — did you do anything forensically
15 to check these devices, or were they simply handed over
16 to the United States?

17 A. No, because we are talking about the M-IAT request,
18 and the case was not conducted at all by Romanian
19 authorities, police or prosecutor's office. We were just
20 fulfilling exactly what was requested in the M-IAT and
21 basically seized the goods and assets and turned them
22 over.

23 So we didn't conduct any type of — that
24 would mean for us to have our own case and to request
25 authorization for the additional forensics from the

Mr. Vaduva - Cross

1 judge, which was not the case.

2 Q. Bagged it up, sent it over?

3 A. Correct. They were untouched from the time we were
4 sealing the apartment until they arrived in the
5 United States.

6 Q. Can an M-IAT request also have you go out and talk
7 to witnesses?

8 A. Yes, of course.

9 Q. And that doesn't require any additional process from
10 a judge. I mean a police officer in Romania can talk to
11 whoever they feel they need to?

12 A. If it is a question that needs a little bit more
13 explaining. So if it is organized crime area of the
14 crime, we only have the prosecutor's office, a special
15 prosecutor's office that only delegates the police
16 officers to do — conduct activities.

17 So us as police, we would not be able to
18 interview a witness, a suspect for anybody without the
19 prosecutor to basically point that out and have a
20 delegation order for us to do that.

21 Q. Okay.

22 A. Because the whole investigation is run by DIICOT.

23 Q. DIICOT is the special prosecutor?

24 A. Yes. The directorate for investigating organized
25 crime and terrorism crimes.

Mr. Vaduva - Cross Cont'd

1 Q. If they give you the order you can talk to whoever
2 is deemed?

3 A. That was named in the delegation.

4 Q. And you can gather up witnesses and have them
5 interviewed if that has been delegated?

6 A. Yes, that is correct.

7 Q. Is there a similar procedure for, say, a Defendant
8 being prosecuted in America who may have witnesses in
9 Romania to request that the Romanian police go find a
10 certain person or certain evidence and send it in a
11 bag?

12 MR. LEVINE: Objection, your Honor.

13 THE COURT: Sustained.

14 BY MR. GOLDBERG:

15 Q. Is there a process where a Defendant, somebody
16 accused of a crime in America, can serve a subpoena that
17 would be processed in Romania?

18 MR. LEVINE: Objection.

19 THE COURT: Sustained.

20 MR. GOLDBERG: I have nothing further.

21 THE COURT: Mr. O'Shea?

22 CROSS EXAMINATION CONTINUED

23 BY MR. O'SHEA:

24 Q. Good afternoon sir.

25 A. Good afternoon.

Mr. Vaduva - Cross Cont'd

1 Q. Do you fly back tonight?

2 A. Yes, 7:45.

3 Q. Very good. If I understood you correctly, sir, you
4 said in connection with your good work at the Romanian
5 National Police starting around 2015, that just from that
6 period of time to when you left, you were involved with
7 hundreds of searches.

8 Did I hear you say that right?

9 A. No. I have said from 2010 since I was employed in
10 that period, I was only working at the directorate for
11 combating organized crime, and since that moment, I was
12 also involved in this case, in particular.

13 Q. How many searches have you done when you were
14 assigned to that unit for, you know, cyber crime if we
15 can call it that?

16 A. I would say less in the period that I was in the
17 directorate because the directorate was handling only the
18 large cases and fewer cases versus the Brigade where
19 actually we didn't conduct only cyber searches.

20 The Brigade was terrorist, combating
21 terrorist, trafficking, human trafficking, migrants and
22 cyber. Because there were so many searches most of the
23 times and also financial investigation unit and because
24 we were a small unit, we were basically helping all of
25 the other colleagues to conduct the searches because we

Mr. Vaduva - Cross Cont'd

1 — there were 24 in our office, a lot more than in the
2 directorate but still not enough?

3 So I was participating in all type of
4 searches, not only cyber. So that's why the number is so
5 high. So there are two or three a week.

6 Q. If we limit it to just cyber crimes during your
7 tenure from 2010 all the way up to the time you joined
8 the DEA, how many a month or year cyber crime searches
9 did you do?

10 A. It would be pretty hard to name exactly, but let's
11 say —

12 Q. More than a hundred; less than a hundred?

13 A. Less than a hundred on cyber.

14 Q. More than 50, less than a hundred?

15 A. I think more than 50.

16 Q. Somewhere between 50 and a hundred.

17 A. Yes.

18 Q. Okay.

19 A. That would be my assumption.

20 Q. All right. Cyber crime is a busy part of your job
21 during that time, fair?

22 A. Very. Every weekend we would have skimming devices
23 in Bucharest, every weekend.

24 Q. Okay. Now, the house — can we see Exhibit 1411?

25 Do you see that picture, sir?

Mr. Vaduva - Cross Cont'd

1 A. Yes.

2 Q. All right. Are you absolutely sure, sir, as you sit
3 here this afternoon that that is the house that you
4 searched that day?

5 A. I believe so.

6 Q. Okay.

7 A. It has been two and-a-half years.

8 Q. Do you know what color Mr. Radu Miclaus's parents'
9 house is?

10 A. No.

11 Q. Okay. Do you know what color the roof is?

12 A. No. As I said, it has been two and-a-half years. I
13 don't think anybody could remember exactly that.

14 Q. Of these routers that we have set up in front of us
15 here, first of all, even in Romania, is possession of a
16 router illegal?

17 A. No.

18 Q. Is possession of a hundred routers illegal?

19 A. No.

20 Q. Okay. Do you know what a log is when it comes to a
21 router?

22 A. Yes.

23 Q. As part of your investigation, did you obtain any
24 logs from these routers?

25 A. Yes. These particular ones?

Mr. Vaduva - Cross Cont'd

1 Q. Yes, sir.

2 A. Oh, no. I thought in general.

3 Q. Do you know what, if anything, these routers
4 were connected to when you went into and searched the
5 house?

6 A. No.

7 Q. Okay. Now, do you remember — we had a couple of
8 side bars on this about this document that — this
9 Exhibit 1414 that was the search — we in America call it
10 a search warrant return report or something of that
11 nature.

12 The handwriting that we saw on the Romanian
13 version of that document, that's all your handwriting.
14 Am I right about that, sir?

15 A. Yes.

16 Q. Now, you don't want these folks on the jury to think
17 that is Radu Miclaus's handwriting, do you?

18 MR. LEVINE: Objection.

19 THE COURT: Sustained.

20 BY MR. O'SHEA:

21 Q. Just so we are clear, that handwriting was not Radu
22 Miclaus's handwriting where blanks are being filled in.
23 That's your handwriting, right?

24 A. Yes. The only — the procedure point for them to
25 sign, they didn't write or make any comments themselves.

Mr. Vaduva - Cross Cont'd

1 Even if you had something to object, I would be the one
2 writing it, and the colleague wrote it for his apartment,
3 and I wrote it for the father's house.

4 Q. And just so I understand your testimony correctly,
5 the only handwriting on that document that is purportedly
6 Mr. Miclaus' is where he signed at the bottom of a page,
7 right?

8 A. Yes.

9 Q. Everything else is either preprinted or your
10 handwriting. Am I correct?

11 A. Yes. And in addition, he also gets a copy to keep
12 up for himself to remain in the house.

13 Q. I thought you had a plane to catch, so let me ask
14 you this.

15 MR. LEVINE: Objection, your Honor.

16 THE COURT: Sustained.

17 BY MR. O'SHEA:

18 Q. The question I asked you, was all the handwriting on
19 that form yours with the exception of Mr. Miclaus'
20 signing at the bottom, right?

21 A. Yes. This is the standard procedure and legal
22 procedure in Romania.

23 Q. Okay. Fifth time I heard you say that. Thank
24 you, sir.

25 MR. O'SHEA: Nothing further.

1 MR. LEVINE: No redirect, your Honor.

2 THE COURT: Sir, you may step down.

3 Ladies and gentlemen, I believe we will take
4 our afternoon recess now. Please remember the
5 admonition.

6 All rise for the jury.

7 (Recess had.)

8 THE COURT: Please be seated. Call your
9 next witness.

10 MR. BROWN: Thank you, your Honor. The
11 United States calls the Special Agent Ryan Macfarlane.

12 RYAN MACFARLANE
13 called as a witness by and on behalf of the Government,
14 being first duly sworn, was examined and testified
15 as follows:

16 DIRECT EXAMINATION

17 BY MR. BROWN:

18 Q. Would you please state your name for the
19 record?

20 A. My name is George Ryan Macfarlane.

21 Q. And what do you go by?

22 A. Ryan.

23 Q. And by whom are you employed?

24 A. I am employed by the FBI.

25 Q. And for how long have you been with the FBI?

1 A. Just over 15 years.

2 Q. And what is your current assignment with the
3 FBI?

4 A. I am a supervisory special agent with the FBI.

5 Q. And where are you assigned?

6 A. I am based here in Cleveland.

7 Q. And what squad do you supervise?

8 A. I supervise a squad called CY 1, which is the
9 national security cyber squad.

10 Q. And how long have you been the squad supervisor of
11 CY 1?

12 A. For about two and-a-half years.

13 Q. And how long total have you been in Cleveland?

14 A. I have been in Cleveland for a total of ten years.
15 However, in the middle of that for about two years I was
16 back in D.C.

17 Q. And before becoming an SSA — is that the correct
18 acronym?

19 A. Yes.

20 Q. Before becoming an SSA, what were your duties?

21 A. My duties, I was a special agent investigating cyber
22 crime.

23 Q. And during your two years in Washington, what did
24 you do?

25 A. While I was in Washington, I was a supervisory

1 special agent, and I was working at the National Computer
2 Investigation Joint Task Force, which is a joint task
3 force that consists of about 15 Government agencies
4 working significant cyber crime and national security
5 matters.

6 Q. And what were your duties there as a supervisory
7 special agent?

8 A. I was managing a region of the country, so I was
9 responsible for approximately eight different offices.
10 And I was overseeing the cyber threats that those offices
11 worked.

12 Q. Now, while you were in Cleveland as a special agent,
13 what were your duties as a special agent investigating
14 cyber crime?

15 A. I was just investigating cases.

16 Q. Okay. And what sorts of cyber crimes did you
17 investigate?

18 A. I investigated a large range of cyber crime,
19 everything from ransomware to internet fraud to computer
20 intrusions, to bank intrusions, and I also worked some
21 state-sponsored intrusions, which would be like China
22 compromises a U.S. company or Russia targets a clear
23 defense contractor.

24 Q. And where were you assigned before coming to
25 Cleveland?

1 A. I was in the Los Angeles field office.

2 Q. And where were you before Los Angeles?

3 A. I was in Atlanta.

4 Q. And what did you do in Los Angeles?

5 A. In Los Angeles, I was doing the same job. I was a
6 special agent investigating cyber crime.

7 Q. And how about Atlanta?

8 A. Atlanta, I lived there before I was part of the
9 Bureau.

10 Q. So your first assignment was in LA?

11 A. It was, yes.

12 Q. What did you do before joining the FBI?

13 A. I did a number of different jobs, but the one I did
14 right before joining the Bureau was, I worked for a small
15 internet security company.

16 Q. Okay. And what did the — what did that company do,
17 what kind of work did it do?

18 A. We helped our clients secure their networks, and I
19 was specifically responsible for managed services, which
20 was basically we watched our clients' networks for signs
21 of malicious activity, hacking.

22 Q. And where did you go to college?

23 A. I went to Georgia Tech.

24 Q. What did you major in at Georgia Tech?

25 A. Computer science.

1 Q. And what sorts of classes did you take as a computer
2 science major?

3 A. I took a wide variety of programming classes, math
4 classes, some engineering classes.

5 Q. Okay. Do you know any computer programming
6 languages?

7 A. Yes.

8 Q. Which languages do you know?

9 A. I know Python. I know C. I know a wide variety of
10 web-based scripting languages and some older languages
11 that have no real relevance to this case.

12 Q. And have you ever written computer programs?

13 A. I have, yes.

14 Q. Have you ever read code?

15 A. Yes.

16 Q. Have you written code?

17 A. Yes.

18 Q. Now, going back to the FBI, what are some of
19 your other duties as a squad supervisor of a cyber
20 squad?

21 A. So as a supervisor of the cyber squad, I am
22 responsible for a team of special agents, analysts, and
23 computer scientists. I — you know, my primary role
24 there is to help them navigate their cases and make sure
25 they have the resources that they need to get their job

1 done.

2 Additionally, I also, as part of my job,
3 have to — am responsible for public engagement.

4 So I spend a lot of my time reaching out to
5 local companies, community groups to explain the types of
6 threats we are seeing and how to best protect yourself
7 against those threats.

8 Q. And why do you provide — is that commonly called in
9 the FBI outreach?

10 A. Yes.

11 Q. Why do you perform outreach in the cyber squad.

12 A. I personally do it because I think it is the right
13 thing to do, but I think it is a needed function of the
14 FBI to make sure the public sees and understands the
15 threats that are out there.

16 Q. And what sorts of outreach programs have you
17 presented?

18 A. I have presented at a large range of the events.
19 I have presented everything from events at local
20 schools, high schools, senior groups. I have talked
21 to local information technology groups, law firms, talked
22 to hospitals talked to retailers. I have presented at
23 real estate conferences, really the entire gamut of
24 events.

25 Q. Fair to say public and private sectors?

1 A. Absolutely.

2 Q. And do you receive any regular training on cyber
3 issues?

4 A. I do. I receive training — usually, I will attend
5 one or two training classes a year time permitting.

6 Q. And in your 15 years of working cyber in the FBI,
7 have you seen any changes as to how the FBI investigates
8 cyber crime?

9 A. Yes, many.

10 Q. Could you explain some of them?

11 A. So for the past 15 years, I would say that what the
12 FBI is seeing with cyber crime is, we are seeing more and
13 more complex cyber crime, and what that means is that we
14 have got groups that are becoming more sophisticated, and
15 there are certain technologies that have changed the
16 landscape of the cyber crime domain essentially?

17 So we have technologies such as dark
18 markets, which are essentially like the Amazon of
19 criminal activity, where criminals can go on those
20 markets, and they can buy and sell the fruits of their
21 labor.

22 One of the big issues cyber criminals had,
23 it was tough to find enough people to find the data that
24 they stole, and dark markets have solved that problem for
25 the cyber criminals. We have seen the rise of

1 cryptocurrency, which is in itself not a criminal
2 technology, but one of the groups that has adopted
3 cryptocurrency is the cyber crime undergrounder because
4 it is a perfect mechanism for laundering money in a
5 semianonymous way?

6 So we are dealing with those kinds of
7 problems, and usually those problems deal with a lot of
8 data. So the FBI is consistently working on how to
9 address that data and how to analyze the data as fast as
10 possible.

11 Q. Now, as a special agent in a cyber squad and now a
12 supervising special agent, what sorts of investigative
13 measures do you or your squad use to investigate cyber
14 crime?

15 A. From an investigation standpoint, we will use all —
16 like a wide range of investigative measures. We will use
17 legal processes, so we will issue subpoenas. We will
18 issue search warrants.

19 We will engage with the private and public
20 sector, both understanding what those groups are seeing
21 out there as well as providing alerts related to what we
22 are seeing.

23 We will engage with other law enforcement
24 around the world because one of the biggest issues with
25 cyber crime is it is worldwide.

1 With cyber crime, you can have a group in
2 Spain or Romania targeting the entire world and using
3 infrastructure around the entire world. So we have to
4 engage with partners globally to address those types of
5 issues, data intercepts.

6 Q. And what do you mean by data intercepts?

7 A. A data intercept is what is equivalent to a wiretap
8 on a phone but just for a server. So instead of
9 listening to phone calls, you are actually seeing the
10 communications that are going inside and outside of the
11 server.

12 Q. Do you use a technique called a pen register trap
13 and trace?

14 A. Yes.

15 Q. Is that sometimes shortened to a pen —

16 A. P-R-T-T, and that's similar to a wiretap, except you
17 don't get to see any of the content. It is just the
18 connection details.

19 So for example, if you did a PRTT or pen
20 trap and trace on an e-mail account, you would see the
21 "from" address and "to "address, the time, and some
22 additional data occasionally but no content.

23 Q. And how do the pen or PRTT differ from a T-III or a
24 wire?

25 A. When you have a wire, you would see all the traffic

1 or all the data that is flowing between that computer and
2 the rest of the world.

3 Q. And in your 15 years with the FBI, approximately how
4 many PRITs have you reviewed?

5 A. I would estimate 50.

6 Q. And how many searches, search warrants have you
7 executed as an agent or special agent?

8 A. Hundreds.

9 Q. And of those hundreds, how many were related to
10 cyber issues or cyber seizures?

11 A. Nearly all of them.

12 Q. And have you ever conducted a cyber wire?

13 A. Yes.

14 Q. Now, did there come a time in 2013 when you were
15 assigned a case involving the Bayrob Group?

16 A. Yes.

17 Q. And when you joined the investigation, what did you
18 understand that investigation to be about?

19 A. So in 2013, I was coming back from Washington, D.C.
20 to Cleveland, and when I arrived here, there was a case
21 that needed some assistance, and it was the Bayrob
22 investigation. I reviewed the data in the case file and
23 understood that back in 2007 —

24 MR. GOLDBERG: Objection.

25 MR. O'SHEA: Objection.

1 THE COURT: Sustained.

2 THE WITNESS: Viewing the case file
3 identified in 2007, there was a local victim in Cleveland
4 that had — was infected —

5 MR. O'SHEA: Object.

6 THE COURT: Sustained.

7 BY MR. BROWN:

8 Q. Were you able to review prior investigative
9 techniques?

10 A. I was, yes.

11 Q. And from that review of the prior investigative
12 techniques, what, if anything, did you learn?

13 A. The case was related to a computer virus or Trojan,
14 and that computer virus was responsible for —

15 MR. GOLDBERG: Objection.

16 THE COURT: Overruled at this point.

17 A. The computer virus was responsible for supporting
18 eBay fraud.

19 Q. Had you at this point in your career investigated
20 any cases involving eBay fraud?

21 A. Yes.

22 Q. Based on that experience, were you familiar with
23 common techniques used in eBay fraud?

24 A. Yes, I was.

25 Q. What did you understand eBay fraud in your

1 experience to be?

2 A. The traditional form of eBay fraud would be where an
3 individual or group would post fake listings on eBay or
4 Craigslist and use the eBay brand to make the fraud look
5 legitimate.

6 Traditionally, though, those fraud cases,
7 internet fraud cases didn't involve any type of virus or
8 malware.

9 Q. And based on your review of the case file and based
10 on your knowledge of traditional eBay fraud, based on
11 your experience, did this appear to be traditionally eBay
12 fraud?

13 A. No. This seemed to be a different type of eBay
14 fraud.

15 Q. What made this different than what you encountered
16 in the past?

17 A. It was more sophisticated.

18 Q. How was it more sophisticated?

19 A. It was the first internet fraud I had seen that
20 involved a Trojan or virus components to it.

21 Q. And what do you understand a Trojan to be?

22 A. A Trojan is a piece of malicious software that is
23 usually packaged with something that purports itself to
24 be legitimate.

25 So an example could be a calculator

1 application that you could download from the internet
2 that would actually be a calculator when you opened it up
3 and ran it on your background, but in the background, it
4 would be installing something malicious.

5 Q. And based on your experience and also your review of
6 the investigation, when you joined the case, how did you
7 understand the Bayrob operation Trojan to operate?

8 A. My understanding of the Bayrob Trojan was that it
9 was related to fraudulent listings posted on eBay, and
10 individuals interested in that vehicle would basically
11 express that interest by bidding or by e-mailing with the
12 person who posted that listing?

13 And then, they would receive a second chance
14 offer that would typically include pictures of the
15 vehicle in the form of a picture viewer, a Kodak picture
16 review, and there was — there is another picture viewer
17 as well?

18 And that picture viewer was a Trojan that
19 would infect the system at the same time, and once
20 infected, that computer would see different content when
21 visiting eBay and other sites on the internet.

22 Q. And based on your understanding of that malicious
23 software, that Trojan, what was your approach to this
24 case when you joined the investigation?

25 A. So my approach to this case was to look at it from

1 two different paths. The first path was like the
2 traditional path of investigating things like
3 interviewing victims, following the money, doing database
4 searches, trying to find someone who had actually spoken
5 to one of the people responsible for this, and the other
6 path was to look at the actual technical component of
7 what the virus was doing, what it was communicating with,
8 and where it was getting his commands from. So there was
9 the traditional path and the technical path, if you
10 would.

11 Q. Is it fair to say the people path and data path?

12 A. Yeah. I would say people/money path and the
13 technical path.

14 Q. And I am sorry, I didn't expect — could you speak a
15 little louder? Did you say technical or tactical?

16 A. Technical.

17 Q. Okay. Sorry.

18 Now, have you described the technical path?
19 What investigative steps did you identify at the
20 beginning of the investigation that were being taken at
21 that time?

22 A. So at the time I joined the investigation, I
23 understood that a number of techniques had been tried to
24 follow the money. There were a number of financial
25 payments that had been sent by victims of the Bayrob

1 Trojan —

2 MR. O'SHEA: Object.

3 THE COURT: Overruled.

4 A. There were a number of financial transactions that
5 had been sent from victims of the Bayrob Trojan to
6 individuals in the U.S. We had identified those victims
7 in the U.S., and we had attempted to follow where those
8 payments went.

9 Q. And how did you trace that money?

10 A. Using legal process, so we would issue legal process
11 to Western Union, for example.

12 Q. And how did that process help the investigation?

13 A. It really — it didn't provide us with any
14 information related to the identities of the people that
15 were responsible.

16 Q. What, if anything, did you learn from this
17 process?

18 A. We learned that the payments were going to Eastern
19 Europe in places like Romania and places surrounding
20 Romania.

21 Q. And how did learning that not help identify
22 anybody?

23 A. The payments were picked up by individuals using
24 fake IDs.

25 MR. O'SHEA: Objection.

1 THE COURT: Overruled.

2 BY MR. BROWN:

3 Q. Now, what other process did you use other than
4 tracing the money?

5 A. So we interviewed victims, but unfortunately, the
6 victims really didn't know who was victimizing them. We
7 interviewed some of the intermediaries, the money mules
8 receiving money from the victims, and sending that money
9 on.

10 But they didn't really have a whole lot of
11 information on who they were speaking with and who they
12 were taking orders from.

13 Q. What, if anything, were you able to learn from
14 interviewing victims?

15 A. We learned there were a —

16 MR. O'SHEA: Objection.

17 THE COURT: Sustained.

18 THE WITNESS: I learned that there were —

19 THE COURT: One moment.

20 BY MR. BROWN:

21 Q. What, if anything, did you learn from interviewing
22 victims?

23 A. I learned that there were a number of —

24 MR. O'SHEA: Objection.

25 THE COURT: Sustained.

1 BY MR. BROWN:

2 Q. What other processes did you use during part of the
3 investigation?

4 A. So other than the people path, if you will, the
5 technical path, what we did was that early on in the
6 investigation we met with Symantec and AOL who had been
7 looking at this problem related to the Bayrob Trojan?

8 And they provided the FBI with data that we
9 analyzed.

10 Q. And at that time, were you using any of the other
11 legal techniques you had testified about earlier?

12 A. At that time, yes. We were issuing subpoenas, and
13 we were doing search warrants on some of the accounts
14 around that time period.

15 Q. And what, if anything, were you learning from those
16 legal processes?

17 A. We were learning that a lot of the accounts just
18 wouldn't have information that we could use to identify
19 who these individuals were. All the technical details
20 were leading to dead ends.

21 Q. What, if anything, did the meetings with — that you
22 had help the investigation?

23 A. So when we met with both Symantec and AOL, they
24 provided us data based on investigations they were
25 conducting on this group.

1 They provided us with the raw data from
2 their investigations, and I took that data and analyzed
3 it myself.

4 Q. And what did you learn from that analysis, if
5 anything?

6 A. So from that analysis, I learned that the
7 Bayrob Trojan was a pretty interesting threat. So it was
8 doing some interesting things to me at least.

9 Q. Based on your training and experience, what did you
10 mean by "interesting things"?

11 A. When I say "interesting," it was designed in a way
12 that I thought was pretty elegant for the period of time,
13 and it was allowing systems to be controlled by this
14 group in a number of different ways.

15 Q. You just used the term "elegant."

16 Does that have a meaning based on your
17 training and experience?

18 A. It was well designed for the time.

19 Q. Now, based on your — on analyzing that information,
20 what steps did you take next?

21 A. So based on that information, I was able
22 to review the data and identify a number of servers
23 that were responsible for controlling the infected
24 systems.

25 Q. And how was that information helpful to your

1 investigation?

2 A. So I took that — those servers, and I issued legal
3 process on those servers and was able to obtain search
4 warrants on those systems.

5 Q. And what, if anything, did you learn from those
6 search warrants?

7 A. So from the search warrants when I received the data
8 back from the providers, I identified that the servers
9 were, in fact, command and control servers for the Bayrob
10 botnet.

11 MR. O'SHEA: Objection.

12 THE COURT: Sustained.

13 BY MR. BROWN:

14 Q. Did you receive information back from the search
15 warrants you issued?

16 A. I did, yes.

17 Q. And were you able to analyze that information?

18 A. Yes, I was.

19 Q. Were you able to analyze that information in regards
20 to investi — was it relevant to the investigation?

21 A. Absolutely, yes.

22 Q. How was it relevant to your investigation?

23 A. The servers I received data on —

24 MR. O'SHEA: Objection.

25 THE COURT: Overruled. I will allow

1 that. Keep going.

2 A. The results of the search warrant identified
3 thousands of files that were — that when analyzed, I
4 identified as being directly related to the Bayrob
5 virus.

6 Q. How were you able to identify those files related to
7 the Bayrob virus?

8 A. So I went through all the files and reviewed the
9 actual code that was contained within the file structure,
10 and I could see, based on the data I received from
11 Symantec and AOL and files and structure on the server,
12 matched essentially. I was seeing two halves of a
13 whole.

14 Q. Now, based on your investigation, approximately how
15 many command and control servers did you identify?

16 A. Over the course of my investigation, I would
17 estimate that I identified approximately ten command
18 control servers that were operating in the U.S., and I
19 was aware that there were other ones that I could not
20 identify.

21 Q. And based on your analysis, were you able to tell if
22 they were all operating at the same time?

23 MR. O'SHEA: Objection.

24 THE COURT: Overruled. You may answer that.

25 THE WITNESS: No. The command and control

1 servers would be active at different periods of time, so
2 they would — from time to time, the command and
3 control server would move from one computer to another,
4 one server to another on the internet, and sometimes
5 they would move from one server provider to another
6 provider.

7 Q. Now, did you serve any other legal process related
8 to the servers?

9 A. Yes. We served a good deal of legal process related
10 to the servers. We would serve pen register trap and
11 traces. We would serve search warrants. We would serve
12 subpoenas, and we also did a data intercept on two to
13 three servers.

14 Q. By "data intercept," you mean a wire?

15 A. Yes.

16 Q. Now, how would doing a wire on a command and control
17 server be helpful to your investigation?

18 A. So doing a wire or data intercept was important for
19 this investigation because the way in which the Bayrob
20 Group had set up their infrastructure made it difficult
21 to investigate.

22 The Bayrob botnet used a tiered approach, so
23 there were infected computers at the bottom. There were,
24 at least, one level of relays, and then there was the top
25 level command and control servers.

1 Q. And how would doing a wire on a server help you see
2 that traffic?

3 A. Because it was the only place that I could see all
4 the infected systems, because if I had a wiretap, for
5 example, on an infected system, it would let me see the
6 communication between that infected system and the relay
7 level?

8 But it would only be the traffic for that
9 one system, whereas if I went all the way up to the top,
10 I would see essentially everything that was connected to
11 the Bayrob botnet.

12 Q. So do you recall the testimony of Liam O'Murchu
13 earlier in this trial?

14 A. Yes.

15 Q. And do you recall the investigation he conducted?

16 A. I do, yes.

17 Q. How is a wire different than the investigation that
18 Mr. O'Murchu testified about?

19 A. So Mr. O'Murchu had data at the infected level. So
20 he had systems that were infected, but they were not at
21 the top level.

22 So he was only seeing a very narrow portion
23 of what was going on, whereas when we got the data
24 intercept at the top level, we could see all the
25 communications between all the different systems.

1 Q. Now, as a wire, I think you testified about what you
2 did to intercept with a wire?

3 A. Yes.

4 Q. What sorts of things did you intercept on a server
5 wire?

6 A. So specifically on this server wire, what I was
7 seeing was I was seeing infected systems check in to the
8 controller, so they would reach out to the controller and
9 say "I am here, hello, do you have any commands for me?"

10 And then, I would see those commands be
11 passed back down, and I would see additional files go
12 down with, you know, with those commands.

13 Q. Were you able to see the content of those files?

14 A. I was, yes.

15 Q. Were you able to see any identities during this part
16 of the investigation?

17 A. During this part of the investigation, I was able to
18 see handles, but they were not accessing the command and
19 control server.

20 Q. And what do you mean by handles?

21 A. Handle would be something that they would use as
22 sort of a criminal alias or nickname.

23 Q. And could you see how they were accessing the
24 command and control server?

25 A. Yes. They were accessing the command and control

1 server in two primary ways.

2 MR. O'SHEA: Object.

3 THE COURT: Overruled. Go ahead.

4 A. The first primary way was through what's called SSH
5 or secure shell, and the second way was through — they
6 were accessing specific files occasionally that were
7 hosted off of that command and control server.

8 One additional aspect was that they were
9 proxying — sometimes they were proxying traffic through
10 the command and control server as well.

11 Q. Okay. What do you mean "proxying traffic through
12 the command and control server"?

13 A. Essentially just relaying traffic through the
14 command and control server.

15 Q. And how can you tell if somebody was proxying
16 through the command and control server?

17 A. For example, on one side, I would see a secure
18 connection come in on one side, and during the time frame
19 of that secure connection, I would see visits to websites
20 out the other end?

21 So I would say a connection come in, and I
22 would see the results of that connection go out.

23 Q. Okay. And how could you see this proxy trafficking
24 in and out using the wire technique?

25 A. So the data interception or wire would show me all

1 the traffic coming across the command and control server,
2 everything, both the secure connections coming in and all
3 the requests to websites going out.

4 Q. Were you able to see it on a computer in the
5 FBI?

6 A. Yes. We have an analysis system that helps to
7 analyze that data.

8 Q. Okay. And using that — is it a computer with a
9 type of software?

10 A. Yes.

11 Q. Okay. So you connect a computer. You are able to
12 see proxy traffic?

13 A. Yes, I was.

14 Q. Could I show you Exhibit 2255? Do you recognize
15 this exhibit?

16 A. Yes.

17 Q. How do you recognize it?

18 A. I made it.

19 Q. When you say you made it, what do you mean?

20 A. I was the one responsible for viewing this traffic
21 and categorizing as well as I was the one that actually
22 made the spreadsheet.

23 Q. Did you create the data within the spreadsheet?

24 A. No. The data was from the data intercept.

25 Q. And did you review all the data you put in the

1 spreadsheet?

2 A. Yes.

3 Q. And is the data a fair and accurate compilation of
4 the data that you observed?

5 A. It is, yes.

6 Q. Now, could we go down to row 275? Do you see
7 725?

8 A. Yes.

9 Q. What is — what are we looking at in row 725?

10 A. This is an event that occurred over the command and
11 control server.

12 Q. What do you mean by an event over the command and
13 control server?

14 A. It was something that I observed that happened
15 over the command and control server that I found
16 interesting.

17 Q. Okay. And can you tell on what date you observed
18 this?

19 A. 3-18-2013.

20 Q. And can we scroll to the right to see rows E through
21 whatever else? Okay. And what is in column E?

22 A. Column E is the date and time.

23 Q. Okay. What does column F tell you, if anything?

24 A. It is a category of the traffic or data.

25 Q. And what does column H tell you, if anything?

1 A. H is empty.

2 Q. Sorry. I.

3 A. I is the website that was visited.

4 Q. And could you tell who visited that?

5 A. Someone with access to the command and control
6 server, but I could not tell specifically who it was,
7 no.

8 Q. How could you tell if it was someone that accessed
9 the command and control server?

10 A. Because this command was sent through it.

11 Q. As part of your investigation, are you familiar with
12 what Ypool.net is?

13 A. Yes.

14 Q. And based on your investigation what is Ypool.net?

15 A. Ypool.net is a website related to cryptocurrency
16 money.

17 Q. And can we keep scrolling to the my left — the
18 other way. Okay. What, if anything, does column M tell
19 you?

20 A. That would be the browser identification of that
21 request.

22 Q. So what does that tell you specifically about
23 the —

24 A. Just the type of browser that was sent with the
25 request.

1 Q. Now, based on your knowledge and investigation of
2 the case, why was a proxy visit to Y pool of
3 investigative importance?

4 A. Because I had seen Ypool before on a Twitter page
5 associated with the handle Radu SPR, which was associated
6 with the criminal handle on Minolta 9797.

7 Q. Now, what other traffic could you see using the
8 wire?

9 A. I saw a lot of criminal activity, so I could see the
10 — I could see infected systems receive commands from the
11 controller that would instruct those infected systems to
12 collect credit card information.

13 MR. O'SHEA: Objection.

14 THE COURT: Overruled.

15 A. And I would see the responses from those infected
16 systems containing credit card information.

17 Q. How could you tell request and responses?

18 A. The data — once analyzing the data, you could see,
19 based on the specific request and format of the data, if
20 it is a request or response?

21 And based on my analysis, I reviewed all the
22 code and I understood exactly how the Trojan worked in
23 relation to the command and control server.

24 Q. Okay. Could you for the time being take 2255 down?

25 Now, could we also take a look at lines 14

1 through 16 of 2255? Was that additional traffic you
2 reviewed?

3 A. Yes, it was.

4 Q. Based on your review, was that traffic of
5 investigative relevance to you?

6 A. Yes, it was. As you can see right here, the command
7 and control server visited a domain at Yahoo related to
8 web posting, and investigation of that website led me to
9 understand that that was —

10 MR. O'SHEA: Objection.

11 THE COURT: Overruled.

12 A. — someone on the command and control server
13 registering a domain at Yahoo.

14 Q. And how was that information of importance to your
15 investigation?

16 A. The Bayrob virus used domains to establish
17 communication between infected systems and the command
18 and control server, and a large number of those domains
19 were registered over small business .yahoo.com.

20 Q. Looking at line 17, did you review that line?

21 A. I did.

22 Q. And was that of investigative relevance to you?

23 A. It was.

24 Q. And can you explain why that was relevant?

25 A. So this specific file ping-view right here is a file

1 that was created by the Bayrob Group.

2 MR. O'SHEA: Objection.

3 THE COURT: Sustained.

4 BY MR. BROWN:

5 Q. Based on your review of this wire data, were you
6 able to compare — were you able to compare this with
7 wire data to other facts you learned during your
8 investigation?

9 A. Yes.

10 Q. Were you able to see any of the data mentioned in
11 this line in other parts of your investigation?

12 A. Yes, absolutely.

13 MR. O'SHEA: Objection. Yes or no answer.

14 A. Yes.

15 Q. And how was that analysis able to help your
16 investigation?

17 A. This file ping-view .PHP was a file that was on the
18 command and control server based on search warrant
19 results I received from the hosting provider. I reviewed
20 this file and understood what it did and also saw it
21 being accessed over the data intercept.

22 Q. Now, what did you understand, based on your
23 investigation, ping-view to do?

24 MR. O'SHEA: Objection.

25 THE COURT: Overruled.

1 A. Ping-view provided a view of all the infected
2 systems and provided some additional capabilities to
3 control those systems.

4 Q. How was an application like ping-view helpful to
5 understand in your investigation?

6 A. Ping-view was a tool that the operators of this
7 server used to manage the infected systems.

8 Q. And why is that an investigative important fact for
9 you?

10 A. Because it is important to understand how these guys
11 operated.

12 Q. Were you able, in analyzing this wire traffic, to
13 also see how many infected systems were being looked at
14 in ping-view?

15 A. Yes.

16 Q. Now, could you take a look at Exhibit 1137? Do you
17 recognize this?

18 A. Yes.

19 Q. How do you recognize it?

20 MR. O'SHEA: Objection. It is being
21 published.

22 THE COURT: Overruled. Pardon me.

23 MR. O'SHEA: Is it published to the jury
24 yet?

25 THE COURT: It is.

1 MR. O'SHEA: Objection.

2 MR. BROWN: May I continue?

3 THE COURT: You may.

4 BY MR. BROWN:

5 Q. How do you recognize this?

6 A. As part of my investigation, I took the data from a
7 command and control server that I did search warrants on,
8 and I recreated the command and control server. I ran my
9 own that was not connected to the internet and was not
10 connected to infected systems.

11 So I took all the data from the search
12 warrant and essentially rebuilt the system so that I
13 could run what they were running.

14 Q. And is this data — is it a fair and accurate
15 recreation of the data you got in search warrant
16 returns?

17 A. Yes.

18 Q. And what does it show to you?

19 A. So this shows one of the interfaces that was built
20 by this group.

21 Q. What does that mean?

22 A. It is a web page used to control infected
23 systems.

24 Q. And where did you find this web page?

25 A. It was on the command and control server in a

1 specific directory with a large number of other files
2 that were related to the Bayrob structure.

3 Q. And looking at Exhibit 1137, were you able to tell
4 how it worked?

5 A. Yes. And I could also see the underlying code
6 behind this. So I could see the interface like the web
7 page it created, but I could also see the logic on the
8 back side of how it worked.

9 MR. BROWN: Your Honor, may I publish this
10 for the jury?

11 THE COURT: Mr. Goldberg, any objection?

12 MR. GOLDBERG: No objection.

13 THE COURT: Mr. O'Shea?

14 MR. O'SHEA: Same objection, Judge.

15 THE COURT: The same objection you said?

16 MR. O'SHEA: Yes.

17 THE COURT: Well, then, I think we need a
18 side bar.

19 (Side bar held on the record.)

20 MR. O'SHEA: Not enough foundation,
21 publicizing. I don't think there has been enough
22 foundation and explanation of what this is before
23 publication to the jury.

24 THE COURT: Well, I am going to be real
25 blunt with you. I am lost, and I don't know if it is

1 because I am not feeling well, but I am lost so I am
2 going to require more foundation so I can understand
3 it.

4 MR. BROWN: All right.

5 (Side bar concluded.)

6 BY MR. BROWN:

7 Q. Special Agent Macfarlane, looking at Exhibit 1137,
8 where did you find this data?

9 A. So this data was on — from the results of the
10 search warrant on the command and control server.

11 Q. Do you recall which command and control server?

12 A. This data was on almost every command and control
13 server I did a search warrant for.

14 Q. So this web page was something you saw in every
15 search warrant return?

16 A. The file ping-view, yes, was nearly on every command
17 and control server I did a search warrant on.

18 Q. And where on the command and control server would
19 you find this page?

20 A. It would be in a subdirectory of the user directory
21 S3, which was the directory that contained a large number
22 of directories and subdirectories that all related to the
23 Bayrob structure.

24 Q. Did you create the data in Exhibit 1137?

25 A. No.

1 Q. Did you populate any of the data in 1137?

2 A. No.

3 Q. Did you create any of the format in 1137?

4 A. No.

5 Q. Is 1137 a fair and accurate representation of
6 the data you found on the search warrant return of a
7 server?

8 A. Yes.

9 Q. And is it a fair and accurate representation of the
10 ping-view you found on every server you issued a search
11 warrant for?

12 A. Yes.

13 Q. Okay.

14 MR. BROWN: Your Honor, may I publish?

15 MR. O'SHEA: Fine, Judge.

16 MR. BROWN: Thank you.

17 BY MR. BROWN:

18 Q. Looking at 1137, what could you tell — based on
19 your investigation, what could you tell the left column
20 to be?

21 A. So the left column here was an identifier for a
22 specific auto option fraud.

23 Q. How could you tell that?

24 A. Based on my review of the files, on the command and
25 control server, and the underlying data in a database

1 that populated this data. It was the conclusion of my
2 analysis.

3 Q. And where was that database located?

4 A. On the command and control server.

5 Q. And what does the next column tell you, if
6 anything?

7 A. The next column would represent the e-mail address
8 of an infected system or associated with an infected
9 system.

10 Q. Based on your investigation, how did you know that's
11 an e-mail address of an infected system?

12 A. Based on my review of the underlying code and the
13 data contained within the database combined with my
14 understanding of how the scheme worked.

15 Q. And based on your knowledge of the investigation, is
16 it, for example, BJ Ward 17@ATT.net, is that something
17 that would have been sent a second chance offer?

18 MR. GOLDBERG: Objection.

19 THE COURT: Sustained.

20 BY MR. BROWN:

21 Q. Do you know how an e-mail address would appear in
22 that column?

23 A. Data from that column would appear once a system
24 was infected, and I knew how the Bayrob Group was
25 infecting victims. It was through the Trojan picture

1 viewer.

2 Q. Now, there are a series of sort of empty boxes or
3 open boxes in four columns. Do you know what those boxes
4 were based on your investigation?

5 A. I do, yes.

6 Q. And what did you know those boxes to be?

7 A. So based on my review of the underlying code, I
8 could tell what those boxes did.

9 Checking one of those boxes would allow you
10 to issue a command to the associated infected victim. So
11 for example, the column that has a number of checks right
12 here that has the camera would instruct the computer to
13 take screen shots. So the infected computer would start
14 taking screen shots of that system, the desktop of that
15 system.

16 Q. Based on your review of all this data, could you
17 tell how taking screen shots was important to the Bayrob
18 virus?

19 MR. GOLDBERG: Objection.

20 THE COURT: Sustained.

21 Q. Could you tell in your review of the code, could you
22 tell where screen shots went once they were taken?

23 A. Yeah. Screen shots went back to the command and
24 control server.

25 Q. So they remained on the command and control

1 server?

2 A. Yes, they did.

3 Q. Could you tell what the other boxes were for?

4 A. The other boxes, if you checked the other boxes, it
5 would collect different types of data.

6 So for example, if you checked the credit
7 card, which is the column next to the camera, which would
8 be right there, it would start to collect credit card
9 information.

10 Q. Could you tell what the other boxes did?

11 A. They would collect other data like log-in data, and
12 I can't recall what this chat one is. At one point in
13 time, I knew what it did, but at this point, I can't
14 recall what it is.

15 Q. Based on your review of the underlying code, were
16 you able to tell if the data collected be, it a screen
17 shot or credit card data, was that collected
18 automatically then?

19 MR. GOLDBERG: Objection.

20 THE COURT: Overruled.

21 A. Yes. There were two ways in which to instruct the
22 botnet to collect data. You could check one of these
23 boxes, or you could change the underlying database, the
24 data within the database to say, for example, I could
25 change an entire field to "on" effectively, and it would

1 make all the infected systems do something like collect
2 log-in data.

3 Q. Based on your review of the code and your
4 understanding at this point of how the botnet worked, did
5 those two manners automate the collection system of the
6 botnet?

7 MR. GOLDBERG: Objection.

8 THE COURT: Overruled.

9 A. My review of this page would basically show it
10 was a way to make it easy to interact with infected
11 victims.

12 Q. Did you see any other web pages like 1137 in your
13 review of the search warrant data that helped interact,
14 helped the Bayrob interact with infected computers?

15 A. Yes. There were approximately somewhere in the
16 range of 10 to 30 different pages that provided some type
17 of service to the users of this server.

18 Q. Could we take a look at Exhibit 1141 without
19 publishing to the jury right now? And do you recognize
20 that?

21 A. Yes, I do.

22 Q. What do you recognize that to be?

23 A. So this is another one of the files on the command
24 and control server.

25 Q. And how do you recognize it to be a file from a

1 command and control server?

2 A. Based on my analysis of the command and control
3 server and the files contained on it. I found this
4 file in the command and control server, and I analyzed
5 it.

6 Q. Did you create any of the data on this page?

7 A. No, I did not.

8 Q. Did you alter any of the data on this page?

9 A. I did not.

10 Q. Did you do anything to format the data on this
11 page?

12 A. I did not.

13 Q. Is the data on this page and its appearance a true
14 and accurate copy of how it appeared in the search
15 warrant returned data.

16 A. Yes, it is.

17 MR. BROWN: May I publish it to the jury,
18 your Honor?

19 THE COURT: Any objection?

20 MR. GOLDBERG: No objection, your Honor.

21 THE COURT: Thank you.

22 BY MR. BROWN:

23 Q. Special Agent Macfarlane, what did looking at
24 Exhibit 1141 help you in understanding the Bayrob Group
25 in your investigation?

1 A. So this page, this web page is another Bayrob web
2 page used by the group to help them manage their fraud
3 scheme.

4 Q. And how, based on your review of the data how, did
5 it help manage the fraud scheme?

6 MR. O'SHEA: Objection.

7 THE COURT: Overruled.

8 A. So this web page was used by members of the Bayrob
9 Group to view communications with victims.

10 Q. And how did it do that?

11 A. This was essentially a criminal version of web mail.

12 MR. O'SHEA: Object.

13 THE COURT: Overruled.

14 BY MR. BROWN:

15 Q. What do you mean by that?

16 A. So I mean that this interface was specifically
17 designed to support the auto auction fraud that has been
18 previously described.

19 Q. How did it support that?

20 A. So for example: It was an inbox like an e-mail
21 inbox that would track by fraudulent listing, put victims
22 or potential victims that were involved in that specific
23 auto auction.

24 Q. Could you tell what LICI L-I-C-I meant in that
25 second column?

1 A. Yes. That's the identifier for a fraudulent
2 listing.

3 Q. And could you tell the identity of the user of this
4 web application by looking at it?

5 A. This is the view that you would see if you
6 were using this system, this web page as MF or Master
7 Fraud.

8 Q. Okay. And how could you tell or how could
9 you identify MF from Master Fraud looking at this page?

10 A. Based on orel, which is up here where my arrow is.
11 You can see the user equals MF.

12 Q. Were there other examples of the web supported
13 application you saw in the search warrant data?

14 A. Yes.

15 Q. And could we look at, without publishing Exhibit
16 1146, do you recognize this?

17 A. I do.

18 Q. How do you recognize it?

19 A. I found this file on the command and control
20 server.

21 Q. And what do you understand this to be?

22 A. A list of templates used for the auto auction
23 fraud.

24 Q. And where was this found?

25 A. On the command and control server.

1 Q. Did you create any of the data on this?

2 A. I did not.

3 Q. Did you modify any of the data on this?

4 A. No.

5 Q. Did you format any of the data on this?

6 A. No.

7 Q. Did you do anything to change or modify the
8 appearance of this?

9 A. No.

10 Q. Is this page a fair and accurate representation of
11 how the data that was formatted on the command and
12 control server?

13 A. Yes.

14 MR. BROWN: Permission to publish to the
15 jury, your Honor?

16 MR. GOLDBERG: No objection.

17 MR. O'SHEA: No objection.

18 BY MR. BROWN:

19 Q. And Special Agent Macfarlane, what on this page was
20 relevant to your investigation?

21 A. So this page is a list of different templates
22 used by the group to generate e-mails to potential
23 victims.

24 Q. And why is finding this data relevant to your
25 investigation?

1 A. Because this data links all the previous data that
2 we had seen from Symantec and AOL and victims.

3 Q. How?

4 A. Because the templates are the same.

5 Q. What do you mean "the templates are the same"?

6 A. So for example, you see this text up here, you can
7 see that we have seen this — this e-mail or this text
8 before, and down here, for example, on Dropbox, you know,
9 we have seen from previous testimony this specific
10 content.

11 Q. So based on your investigation, what importance did
12 Dropbox mean?

13 A. Dropbox was the service that they were using
14 to send links in the e-mail when they were infecting a
15 victim.

16 Q. And if you look at the box labeled text-2 —

17 A. Yes.

18 Q. — could you explain in the subject why the text
19 looks like that, if you know?

20 A. So when you see the brackets and the carats, this is
21 a way of randomizing the message before it would go out,
22 so that when the Bayrob Group was sending messages, each
23 message would look slightly different, so that it was
24 harder for security companies to generate signatures on
25 it. So this was an evasion technique.

1 Q. And based on your investigation and your experience,
2 why was it important to evade detection?

3 A. This group needed to evade detection to be
4 successful with their fraud.

5 Q. Now, do you see any other web-based templates that
6 are helpful in the fraud scheme?

7 A. I did, yes.

8 Q. Without publishing to the jury, could we take a look
9 at Exhibit 1138? Do you recognize this?

10 A. I do, yes.

11 Q. What do you recognize it to be?

12 A. So this is the view that a member of the Bayrob
13 Group would have when they were on the other end of a
14 live eBay chat with a victim.

15 Q. And where did you find this?

16 A. I found this on the command and control server.

17 Q. Did you create any of the data in this exhibit?

18 A. I did not.

19 Q. Did you modify any of the information in this
20 exhibit?

21 A. I did not.

22 Q. Did you format any of the information in this
23 exhibit?

24 A. I did not.

25 Q. Is this exhibit a fair and accurate representation

1 of the data and the formatting as you saw it on the
2 command and control server?

3 A. It is, yes.

4 MR. BROWN: Your Honor, permission to
5 publish 1138?

6 MR. O'SHEA: No objection.

7 MR. GOLDBERG: No objection.

8 MR. BROWN: Thank you.

9 BY MR. BROWN:

10 Q. Could you explain what you see on this web
11 page?

12 A. So what we are looking at here is a web page
13 that would be used by a member of the Bayrob Group
14 to communicate as an eBay agent over chat with a
15 victim.

16 Q. Based on your investigation, did you see eBay chats
17 anywhere?

18 A. Yes.

19 Q. What was the importance of your investigation to
20 eBay chat?

21 A. EBay chat was a feature of the Bayrob Trojan, so
22 when victims clicked on a Bayrob auto action and hit the
23 "support" or "help" link, they would be redirected to a
24 member of the Bayrob Group instead of being redirected to
25 eBay.

1 Q. And what was the importance based on your
2 investigation of having that functionality?

3 A. This data represents communications between the
4 Bayrob Group and victims.

5 Q. Now, looking at this, who is eBay?

6 A. So in this web page, eBay would be the Bayrob
7 Group.

8 Q. And who would UB be?

9 A. That would be the victim.

10 Q. And in this exhibit who is the UB?

11 A. This would be the victim associated with B. J. Ward
12 17@ATT.net.

13 Q. And how would a member of the Bayrob Group
14 communicate using this template?

15 A. So they would see messages that they had sent and
16 the victim had sent, and then they would type into this
17 box down here their reply, and then they would click the
18 reply-to-asshole button.

19 Q. What do you mean reply to asshole?

20 A. That's just the name of the button.

21 Q. During your investigation, did you ever talk to
22 people at eBay?

23 A. Yes.

24 Q. Did you ever learn if reply to asshole is a
25 functional button for employees of eBay?

1 MR. GOLDBERG: Objection.

2 THE COURT: Sustained.

3 BY MR. BROWN:

4 Q. Was there anything else on this exhibit or this web
5 page that was relevant to your investigation into the
6 Bayrob Group?

7 A. The URL for all of these exhibits is important
8 because I was able to use the URLs and the data structure
9 on the command and control server and match that up with
10 traffic from the data intercept as well as other
11 information in the course of my investigation.

12 All of these files helped me understand how
13 the Bayrob Group did what they did.

14 Q. Special Agent, it is 4:00 p.m. I am going to ask a
15 stepback question.

16 What in the URL was relevant to your
17 investigation?

18 A. The directory structure and the file.

19 Q. Now, when you mean "directory structure," is that
20 basically just a listing of where the file lives on the
21 directory?

22 A. Yes. When you go to a website, the URL will
23 sometimes include where on the website you are going. In
24 this case, there is a corresponding directory on the
25 command and control server in the /S my 4 directory, and

1 the my 4 directory contains a lot of files that help
2 support the auto auction fraud.

3 Q. And you heard testimony about extensions during this
4 trial?

5 A. Yes.

6 Q. Is .PHP an extension?

7 A. Yes.

8 Q. What significance to this case did you place on this
9 .PHP?

10 A. The .PHP in this case was significant because the
11 main files that were responsible for controlling the
12 malware were written in .PHP as well as a number of files
13 that were responsible for collecting a variety of
14 information from infected systems.

15 Q. Now, did you continue your analysis of the wire?

16 A. Yes.

17 Q. Did you also continue your analysis of the search
18 warrant data?

19 A. Yes.

20 Q. What, if anything, did you see in the analysis of
21 those two sources of information?

22 A. So between the data from the interception and the
23 data from the search warrants, I could take those two
24 pieces of data, and I could understand how infected
25 systems used the files on the command and control server,

1 and I found over I think 1400 directories that were
2 related to different aspects of the fraud.

3 Q. I think you testified earlier about the screen
4 shots. Do you recall that?

5 A. I did, yes.

6 Q. Did you find directories with screen shots on the
7 command and control server?

8 A. I did. I found directories containing screen
9 shots.

10 Q. What, if anything, was the importance to your
11 investigation of screen shots?

12 A. The importance of the screen shots based on, if you
13 remember ping-view, you could select the check box that
14 would take a screen shot, and that would tell the virus
15 to take screen shots of the infected system.

16 Those screen shots would then go back to the
17 command and control server and be effectively on the
18 command and control server. It was a way of documenting
19 or seeing what their victims were seeing.

20 Q. Okay. And when you say "screen shots," what do you
21 mean?

22 A. Just a picture of your desktop.

23 Q. Okay. Could we take a look at Exhibit 1170? Let's
24 not publish it yet, make sure there are no objections.

25 Do you recognize that?

1 A. I do.

2 Q. What do you recognize that to be?

3 A. A screen shot.

4 Q. How do you recognize it to be a screen shot?

5 A. Because I know it was found on the command and
6 control server.

7 Q. And did you create any of the data on that screen
8 shot?

9 A. I did not.

10 Q. Did you alter any of the data on that screen
11 shot?

12 A. I did not.

13 Q. Did you modify or format any of the data on that
14 screen shot?

15 A. I did not.

16 Q. Is that screen shot a reliable, fair, and accurate
17 reliable image of the screen shot you saw on the command
18 and control server?

19 A. It is, yes.

20 MR. BROWN: Permission to publish to the
21 jury, your Honor?

22 MR. GOLDBERG: No objection.

23 MR. O'SHEA: No objection.

24 BY MR. BROWN:

25 Q. Special Agent Macfarlane, can you tell us, what are

1 we looking at?

2 A. So this is a picture found on the command and
3 control server.

4 Q. And what is it a picture of if you could tell?

5 A. It is the picture of a desktop of an infected
6 system.

7 Q. How could you tell it is a picture of a
8 desktop?

9 A. I know it is infected because it was found on the
10 command and control server. I analyzed both the related
11 traffic from infected systems as well as the files that
12 were responsible for initiating these types of screen
13 shots on infected systems.

14 Q. And looking at that screen shot, what, if
15 anything, could you tell of relevance to your
16 investigation?

17 A. So based on my understanding of all of the data that
18 I obtained from the search warrants and the data
19 intercept, I understood that this screen shot was a
20 result of an infection?

21 So I knew this was an infected computer
22 because the only way in which this could come on to the
23 command and control server was if the system was
24 infected, because it had to get infected first before it
25 could actually take screen shots for the Bayrob Group.

1 Additionally, each one of these screen
2 shots would have a unique identifier associated
3 with the specific infected system that it came
4 from.

5 Q. Did you find any programs or any code that showed
6 people sending screen shots from the desktop to the
7 command and control server?

8 A. Yes, I did.

9 Q. Of people?

10 A. Of like individuals sending?

11 Q. Yes.

12 A. No, no. This was just a function of the
13 malware.

14 Q. Okay. And looking at this page, what was of
15 investigative interest to you?

16 A. A few things that were of interest to me were some
17 consistencies that I had seen in other places. For
18 example, this was consistent with the templates that I
19 had seen from other sources of the investigation, such as
20 data provided by victims, data provided by AOL and
21 Symantec, as well as other screen shots that were on this
22 command and control server.

23 Q. And Special Agent Macfarlane, what are you pointing
24 at?

25 A. So this is the feedback rating, and if you remember

1 from earlier testimony, this 106 stars is part of the
2 Bayrob template for their fake eBay page or their fake
3 eBay listing.

4 Q. Did you see anything else about this page that had
5 the indicia of being part of the Bayrob Group?

6 A. Yes. And here is the eBay and protection, which was
7 invented by the Bayrob Group.

8 Q. Did you see any other screen shots that were of
9 investigative interest to you?

10 A. I did, yes. There were thousands.

11 Q. If you look at Exhibit 1177 without publishing to
12 the jury, please.

13 Do you recognize this?

14 A. Yes.

15 Q. What do you recognize it to be?

16 A. Another screen shot of an infected system.

17 Q. Where did you find this screen shot?

18 A. I found this screen shot on the command and control
19 server.

20 Q. Did you create this data?

21 A. I did not.

22 Q. Did you add or modify any data to this web page?

23 A. I did not.

24 Q. Did you do anything to change the formatting of this
25 screen shot?

1 A. No. This was just a picture I found on the command
2 and control server.

3 Q. And is this screen shot a fair and accurate
4 representation of what you found on the command and
5 control server?

6 A. Yes.

7 MR. BROWN: Permission to publish to the
8 jury, your Honor?

9 MR. GOLDBERG: No objection.

10 MR. O'SHEA: No objection.

11 BY MR. BROWN:

12 Q. And looking at Exhibit 1177, what, if anything, was
13 of investigative interest in this screen shot?

14 A. So this screen shot showed the desktop of
15 another infected system. I could see up here
16 that someone was logged into their Outlook account under
17 gradyread@hotmail.

18 I could see the current tab, which was a
19 Bayrob Group auction because it had the eBay agent
20 protection, and I could see other things on the desktop
21 such as what programs were on their desk bar down here
22 and the time, for example.

23 Q. And were there screen shots involving other parts of
24 the eBay auction fraud scheme on the command and control
25 server?

1 A. There were. They would take screen shots of almost
2 every aspect of the fraud process.

3 Q. Based on your investigation and review of the wire
4 traffic and the command and control server, were you able
5 to determine what the purpose of the self-documenting
6 through screen shots was?

7 A. My analysis of the command and control server showed
8 that the Bayrob Group kept excellent records of
9 everything they did when it related to interactions with
10 victims.

11 They would track multiple different data
12 points for each investigated system to include screen
13 shots of the infected systems, account listings that were
14 stolen from that system, the way that system was used to
15 register domains or interact with other websites at the
16 direct command of the botnet as well as per victim a
17 large amount of data that was specific to their ability
18 to control all these different systems.

19 Q. And based on that, did you see — could I show you
20 without publishing Exhibit 1180, and do you recognize
21 this?

22 A. I do, yes.

23 Q. What do you recognize it to be?

24 A. Another screen shot of infected system.

25 Q. And where did you find this?

1 A. On the command and control server.

2 Q. Did you create this data?

3 A. Yes, sir.

4 Q. Pardon me?

5 A. No. I'm sorry, no.

6 Q. You did not create this data?

7 A. No.

8 Q. Is this a screen shot?

9 A. It is, yes.

10 Q. Did you alter any of this data?

11 A. I did not.

12 Q. Did you modify any of this data?

13 A. I did not.

14 Q. Is this a fair and accurate representation of what
15 you found on the command and control server?

16 A. It is, yes.

17 MR. BROWN: Permission to publish?

18 MR. GOLDBERG: No objection.

19 MR. O'SHEA: No objection, Judge.

20 BY MR. BROWN:

21 Q. And what of investigative importance did you find
22 from this screen shot?

23 A. So this screen shot is another screen shot of an
24 infected system, and I could see that when the screen
25 shot was taken the infected computer, the user of the

1 infected computer, had agreed to buy the vehicle, and an
2 invoice was generated.

3 Q. How could you tell that?

4 A. I could tell that because I found this specific
5 template on the command and control server, and this was
6 consistent with other data sources on specifically how
7 this scheme was run by this group.

8 Q. And where on the command and control servers would
9 you find those templates?

10 A. In various directories based on what the template
11 was related to.

12 Q. Did you see on this screen shot any other data that
13 would have come from directories on the command and
14 control server?

15 A. Yes. This template was a Bayrob template that I
16 found on the command and control server, and it had other
17 specific data items that I had seen in other places such
18 as fax numbers and victim data as well as, you know, item
19 numbers.

20 All of these things were in the underlying
21 data found on the command and control server.

22 Q. And based on your review of the code, were you able
23 to tell how that data that you pointed out, the victim
24 data, populated those directories?

25 A. Yes. A number of these data items came out of a

1 database that was created by the Bayrob Group.

2 Q. Okay. Now, were you also able to see these sorts of
3 templates in other parts of the fraud scheme?

4 A. Yes.

5 Q. Showing you Exhibit 2701 without publishing, do you
6 recognize this?

7 A. I do.

8 Q. How do you recognize it?

9 A. This is a file that was found on the command and
10 control server.

11 Q. And did you create any of the data?

12 A. I did not.

13 Q. Did you modify any of the data?

14 A. I did not.

15 Q. Did you change any of the formatting?

16 A. I did not.

17 Q. Is this, in fact, a screen shot?

18 A. Yes.

19 Q. Is this a fair and accurate representation of
20 a screen shot you saw on the command and control
21 server?

22 A. No. I took this screen shot after standing up
23 the — like the command and control server.

24 Q. So this is a screen shot?

25 A. It is, yes.

1 Q. But you took the screen shot?

2 A. I took the screen shot, yes.

3 Q. Is this a screen shot a fair and accurate
4 representation of the web page or of the data you found
5 on the command and control server?

6 A. It is, yes.

7 MR. BROWN: Permission to publish, your
8 Honor?

9 THE COURT: Mr. Goldberg?

10 MR. GOLDBERG: No objection.

11 MR. O'SHEA: No objection, Judge.

12 BY MR. BROWN:

13 Q. And looking at Exhibit 2071, what, if anything, was
14 of investigative importance to you?

15 A. So the company or the site name MITPL was of
16 importance because we had seen it in other places in our
17 investigation as a site that was used to recruit what
18 were called mules, which were individuals that received
19 money from victims and then sent them on to other places
20 in Europe.

21 Q. Is it fair to say that this is a recruiting page for
22 money mules?

23 A. It is, yes.

24 MR. O'SHEA: Objection.

25 Q. Based on your investigation, did you recognize this

1 to be —

2 THE COURT: Is there an objection?

3 MR. O'SHEA: Yes.

4 MR. GOLDBERG: Yes.

5 THE COURT: Overruled. I am going to allow
6 the answer to stand.

7 A. Yes. It was a recruiting page.

8 Q. And did you see any other data relevant to your
9 investigation?

10 A. Yes. This page had other indicators that we had
11 seen in data from other aspects of the investigation, so
12 a number of these names, for example, were other
13 recruiting companies that we were aware of that were
14 recruiting mules for the Bayrob Group such as KST.

15 At one point in time, there was a U.S. wire
16 service, and the site name was MIPL, which was another
17 fake company doing recruiting for the Bayrob Group.

18 Q. Okay. Now, was a page like this also drawing
19 information from databases on the command and control
20 server?

21 MR. GOLDBERG: Objection.

22 THE COURT: Sustained.

23 BY MR. BROWN:

24 Q. Okay. Were you able to — seeing a page like that,
25 was there any investigative interest related to the

1 command and control server?

2 A. So, yes. Seeing files such as this one and other
3 files that were on the command and control server, it was
4 apparent to me that whoever was running this command and
5 control server was also running the recruitment
6 operations that we had seen in other aspects of the
7 investigation.

8 Q. Were you able to see directories that supported
9 the recruitment operation on the command and control
10 server?

11 MR. GOLDBERG: Objection.

12 A. Yes.

13 THE COURT: Overruled.

14 A. Yes. They were on the command and control
15 server.

16 Q. And when you say they were directories, what did
17 they look like?

18 A. So a directory is just a folder essentially, which
19 you put files into or other directories.

20 So it would be a listing or a structure of
21 files that would be logically organized to categorize
22 data in a way that meant something to the users of the
23 system.

24 Q. And what would the data within those files look
25 like?

1 A. It would vary. Some of the data would be templates
2 like this. Some of the data would be files that
3 contained information, that would be imported into files
4 like this.

5 Some of the data would be like templates or
6 data collected from web pages like this, such as people
7 that signed up that would provide their information.
8 That data might end up on the command and control server
9 in a directory related to this page.

10 Q. Without publishing to the jury, looking at Exhibit
11 2201, do you recognize this?

12 A. Yes.

13 Q. What do you recognize it to be?

14 A. This is data that was contained within the
15 database.

16 Q. Okay. And how do you recognize it as data contained
17 within a database?

18 A. Because I reviewed all the data in the data base,
19 and this is the data that I saw.

20 Q. And where did you find this data?

21 A. So on the command and control server, there was a
22 database that tracked a large amount of data related
23 to — related to all aspects of the criminal scheme, to
24 include the auction fraud, the recruiting, the money
25 mules, the infected systems, and a number of other

1 aspects. There were over 50 tables related to different
2 information that was tracked and used by the Bayrob
3 Group.

4 Q. And this was found on one of the command and control
5 servers?

6 A. That is correct, yes.

7 Q. Did you create this data?

8 A. I did not, no.

9 Q. Did you modify the data?

10 A. I did not.

11 Q. Did you format this data?

12 A. I did not.

13 Q. Is this a fair and accurate representation of the
14 data as it existed on one of the databases on the command
15 and control server?

16 A. It is, yes.

17 MR. BROWN: Permission to publish 2201?

18 MR. O'SHEA: Can we have a side bar real
19 quick on that one, your Honor?

20 THE COURT: You may.

21 (Side bar held off the record.)

22 BY MR. BROWN:

23 Q. Special Agent Macfarlane, before we go on, did you
24 for a program format this data?

25 A. Yes. I pulled this data out of the database so that

1 we could see it and view it.

2 Q. Did you put it in a format that is legible or
3 readable?

4 A. I did, yes.

5 Q. And in formatting this data, did you change any of
6 the data?

7 A. No.

8 Q. Did you change any of the meaning of the data?

9 A. No.

10 Q. Is this data the same data that existed on the
11 command and control server?

12 A. It is.

13 Q. But in a different format?

14 A. Yes. It is the way in which we can view the data
15 within the database.

16 Q. Okay. Is this an Excel spreadsheet? Do you know
17 which program you used?

18 A. So I used a tool called My Sequel Workbench, which
19 is a tool that allows you to access databases, and it
20 will take the data within a database and allow you just
21 to see it. There is export function of that tool, which
22 allows you to export that data into a text format
23 file, and you can then use that file and view it
24 in a text viewer or Excel or a number of different
25 tools.

1 Q. So you hit export, and it is readable?

2 A. Yes. And then you'd use another tool to read it.

3 In this case, I don't specifically remember what I used
4 to create this, you know, to export and view this data,
5 but it was likely Excel if I had to guess.

6 Q. If you are using would Excel, Special Macfarlane,
7 would comma separating or tab separating the columns make
8 a difference in formatting?

9 A. So that is a different format, yes, because the
10 fields are limited by two different characters, a comma
11 or a tab, but it wouldn't change the rest of the data.
12 You would still be able to import it into Excel and view
13 it or view it using a text viewer.

14 MR. BROWN: Your Honor, I would move to
15 publish at this point that the data has not changed from
16 the database.

17 THE COURT: Mr. Goldberg, any objection?

18 MR. GOLDBERG: No objection.

19 MR. O'SHEA: No objection, Judge.

20 MR. BROWN: Thank you, your Honor.

21 BY MR. BROWN:

22 Q. And could you explain what this table is?

23 A. So this table is data related to recruitment
24 operations that were done by the Bayrob Group. So this
25 first column was a list of infected systems that were

1 used with an associated e-mail account and a password for
2 that e-mail account.

3 So for example, we had seen the Bayrob Group
4 use the alias Martin Steinberg to recruit mules as part
5 of the criminal scheme. This column contains a large
6 number of e-mail accounts that were used or consistent
7 with that alias.

8 Q. And in fact, did you see those e-mail addresses in
9 recruitment pages?

10 A. We did, yes.

11 Q. And what is the SOCKS column, what does SOCKS mean?

12 A. So these columns are named by the Bayrob Group, and
13 this was the name of the column related to infected
14 systems, the port which it connected to and data that you
15 would need to proxy through that system.

16 Q. And were you able to determine in your investigation
17 what the status column meant?

18 A. The status column was information as to the current,
19 whether this e-mail account was still active, good, or
20 working.

21 Q. Okay.

22 THE COURT: Folks, we are going to adjourn
23 for the evening. Do not form any opinion, and do not
24 talk about the case. Please be downstairs tomorrow
25 morning at 9:00 a.m. We will call for you at that time.

1 Have a good evening everybody. All rise for
2 the jury.

3 (Jury out.)

4 THE COURT: Okay. Let's go through the
5 exhibits for the day. Are you offering 1410?

6 MR. LEVINE: No.

7 THE COURT: 1411?

8 MR. LEVINE: Yes.

9 THE COURT: I am just going to start reading
10 now: 1413, 2424.

11 MR. BROWN: Is that a physical?

12 MS. CHANDLER: Yes.

13 MR. BROWN: Okay.

14 THE COURT: 2341.

15 MR. LEVINE: Physical.

16 THE COURT: 2317.

17 MR. LEVINE: Physical.

18 THE COURT: 255.

19 MR. LEVINE: Physical.

20 THE COURT: 1415.

21 MR. LEVINE: Physical.

22 THE COURT: 2047.

23 MR. LEVINE: Physical.

24 THE COURT: 2048.

25 MR. LEVINE: Physical.

1 THE COURT: 2049.

2 MR. LEVINE: Physical.

3 THE COURT: 2050.

4 MR. LEVINE: Physical.

5 THE COURT: 2051.

6 MR. LEVINE: Physical.

7 THE COURT: 2052.

8 MR. LEVINE: Physical.

9 THE COURT: May I assume that you are
10 offering only pages 3, 4, 7, and 8 of 1414?

11 MR. LEVINE: Correct, your Honor.

12 THE COURT: 2054.

13 MR. LEVINE: Physical.

14 THE COURT: 2255.

15 MR. O'SHEA: What was the last one? I
16 apologize.

17 THE COURT: That's all right. 2054.

18 MR. O'SHEA: Okay.

19 THE COURT: 2255, 1137, 1141.

20 MR. O'SHEA: What's 1137? Oh, that. Okay.

21 THE COURT: I will repeat, 1141, 1146, 1138,
22 1170, 1177, 1180, 2071, 2201. On behalf of the
23 Government, did I miss anything?

24 MR. BROWN: I do not believe so, your Honor.
25 I will double check with the expert.

1 Exhibits offered pursuant to a stipulation
2 by Paul Mueller, and we can talk tonight and sort those
3 out.

4 MR. GOLDBERG: Your Honor, I don't think you
5 missed anything.

6 THE COURT: Okay. We will see you in the
7 morning.

8 (Trial adjourned at 4:33 p.m.)

9 - - - -

10 C E R T I F I C A T E

11 I, George J. Staiduhar, Official Court
12 Reporter in and for the United States District Court,
13 for the Northern District of Ohio, Eastern Division,
14 do hereby certify that the foregoing is a true
15 and correct transcript of the proceedings herein.

16
17 s/George J. Staiduhar
18 George J. Staiduhar,
Official Court Reporter

19 U.S. District Court
20 801 W. Superior Ave., Suite 7-184
21 Cleveland, Ohio 44113
22 (216) 357-7128
23
24
25